“SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO”

PRESENTADO POR:
DANIELA BERMEO FIESCO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
PITALITO - HUILA
2020

“SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO”

PRESENTADO POR:
DANIELA BERMEO FIESCO

DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN) INFORME FINAL PARA OPTAR POR EL TÍTULO DE INGENIERA DE SISTEMAS

TUTOR:
HECTOR JULIAN PARRA
MSC. DIRECCIÓN ESTRATÉGICA ESPECIALIDAD TELECOMUNICACIONES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
PITALITO - HUILA
2020

Nota de Aceptación

_____

_____

_____

_____

_____

_____

Pitalito, Huila (13, mayo, 2020) (15, mayo, 2020)

DEDICATORIA

Dedico este proyecto principalmente a Dios, por permitirme cumplir una de mis metas más anheladas en mi vida.

También gracias, por encontrar y cruzarme en el camino a personas maravillosas que han aportado su granito de arena para convertirme en la profesional que soy.

A mis padres por confiar en mis capacidades y virtudes, de creer en mis metas que son metas para ellos.

A mis tutores en la UNAD, que gracias a su apoyo, persistencia y paciencia lograron inspirar en mí un gran sentido de responsabilidad y compromiso conmigo misma y en mi entorno profesional

AGRADECIMIENTOS

En estas líneas quiero agradecer a mis padres por el esfuerzo, dedicación, paciencia, por su confianza y por todo lo que me han dado a lo largo de mi carrera y de mi vida.

Quiero expresar mi gratitud a los tutores de la UNAD Pitalito-Huila, porque siempre estuvieron dispuestos a apoyarme en cada proceso y en el transcurso del desarrollo del proyecto siempre tuvieron la mejor disposición para enseñarme y guiarme por el camino más conveniente para que mi desarrollo profesional sea el mejor.

De manera especial a mis colegas que me animaron cada día y me ofrecieron su apoyo en momentos críticos en el camino de mi carrera universitaria y de seguir cultivando mis valores y capacidades profesionalmente.

TABLA DE CONTENIDO

LISTA DE FIGURAS

RESUMEN

El presente trabajo, consiste en configurar distintos escenarios (escenario 1 y escenario 2), en el escenario 1, se demostrará cada detalle de la configuración, incluido la asignación de direcciones IPv4 e IPv6; para garantizar el enrutamiento de las redes, se utilizó el protocolo RIPv2. Para garantizar la seguridad de los equipos, se asignaron contraseñas de consola, vty y, de modo privilegiado; también, se crea una lista de control de acceso y así evitar intrusiones al momento de usar TELNET; para proporcionar una mayor seguridad, se proporciona el protocolo NAT, así, cuando se realice una petición a una red exterior, este se traducirá y permitirá la conexión hacía la red pública; para asignar las direcciones de forma más fácil, se realiza uso del protocolo DHCP, para que los equipos funcionen correctamente en la red, es necesario que manejen la zona horaria local, para ello se proporciona el servicio NTP y poder dar solución para este caso.

El escenario 2, requería una configuración que le permitiese conectarse desde una red LAN ubicada en MEDELLIN hasta una red LAN ubicada en BOGOTA, para poder dar solución a este problema, se tuvo que configurar un enrutamiento por OSPFv2, para no consumir recursos, se desactivo la propagación del mismo, como seguridad, se configuro el protocolo PPP con autenticación pap y chat, para permitir la conexión entre ciudades se configuro NAT donde el ISP sería la red pública y por último se proporcionó el servicio DHCP para que las LAN contasen con direcciones IP.

PALABRAS CLAVES: configuración, IPv4, IPv6, enrutamiento, OSPF, RIPv2, TELNET, red, VLAN, servidor, lista de control de acceso, protocolo.

1. INTRODUCCIÓN

El trabajo cuenta con 2 redes para realizar su respectiva configuración, se les debe asignar un protocolo de enrutamiento a cada red y determinados servicios; cada subred tendrá comunicación con otras subredes de su red, la única diferencia es que unos equipos contaran con accesos especiales.

En el escenario 1 se utilizará el protocolo de enrutamiento RIPv2, este es un protocolo de enrutamiento dinámico, permitirá conocer rutas hacia otras redes de manera más sencilla; este escenario contara con servicios NTP, DHCP, VLAN, servicios que ayudaran a la asignación de direcciones IP, asignación de hora y fecha y, asignación de red de área local virtual, para una mejor gestión de la red; también contara con el protocolo NAT y con una ACL, esto para traducir las direcciones IP de privadas a públicas y viceversa y, también, para controlar el acceso de los usuarios de la red. Al momento de configurar el escenario 2 se debe tener en cuenta que para este se utilizara el protocolo OSPF, en el cual se manejará la misma referencia de protocolo y la misma área para cada router, también se le asignará un identificador a cada uno y; también contara con un protocolo de encapsulamiento y de autenticación, cada segmento de red manejara una autenticación distinta, sin embargo, permitirá la comunicación de ambos lados; por último se configura un servicio DHCP, que sea capaz de proporcionar direcciones IP de forma dinámica a todos los pc de cada LAN.

2. PLANTEAMIENTO DEL PROBLEMA

2.1 DEFINICIÓN DEL PROBLEMA

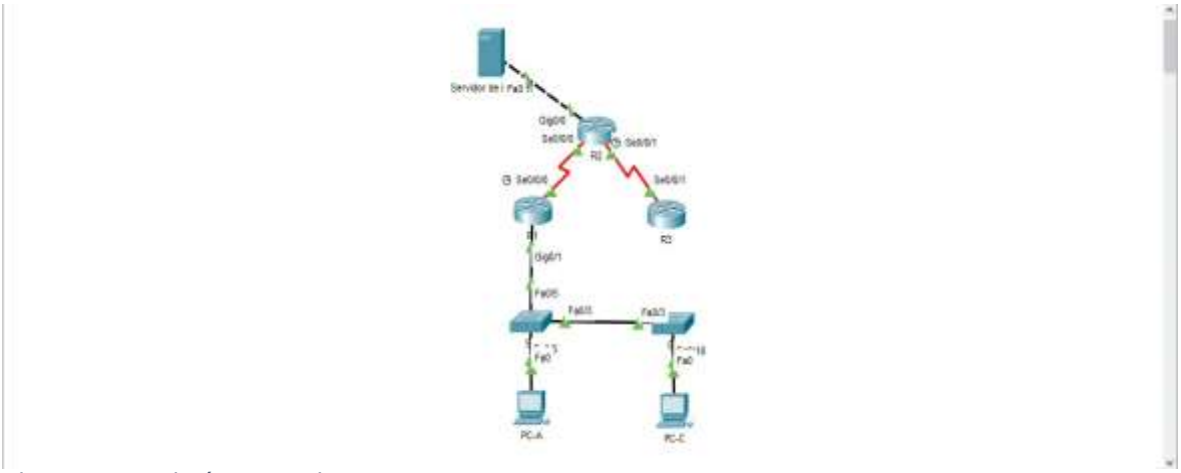
Para este informe se cuenta con 2 escenarios que deben ser configurados desde 0, según las indicaciones proporcionadas; es de importancia solucionar estos 2 escenarios, debido a que si la red no cuenta con los servicios necesarios, puede presentar pérdida de ingresos a la empresa, para ello se debe tener en cuenta los protocolos de enrutamiento, listas de control de acceso, redes de área local virtual, asignación de dirección IP dinámica y otros protocolos que pueden ayudar a mejorar la gestión de la red

2.2 JUSTIFICACIÓN

La solución debe proporcionarse, ya que, en caso de que la red no funcione correctamente, los trabajadores y sus labores no tendrán buenos resultados, afectando a la empresa, luego a las personas que reciben ingresos de estos trabajos y también, afectando a los usuarios del servicio que puede llegar a proporcionar la empresa, para brindar esta solución, se realiza la simulación en el software Packet Tracer, el cual brinda entornos de simulación reales, este software se elige ante otros, debido a su fácil manejo y que no es necesario realizar configuraciones para su uso, solo se configuran los equipos que se van a utilizar.

3. ESCENARIO 1

Escenario1: Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico RIPv2, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Durante la evaluación, probará y registrará la red mediante los comandos comunes de CLI.



Figuras 1. Topología escenario 1

3.1 PARTE 1: INICIALIZAR LOS DISPOSITIVOS

3.1.1 paso 1: inicializar y volver a cargar los routers y los switches

Primero se eliminará el archivo startup-config de los Routers, para ello se utilizan los siguientes comandos:

Router>enable
Router#erase startup-config

Se debe realizar una confirmación para ello se presiona Enter, esto se realiza en todos los routers.

Ahora se vuelven a cargar todos los router, esto con el comando:

Router#reload
Proceed with reload? [confirm]

Para confirmar, solo se presiona Enter.

Ahora se debe eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior; los comandos son:

Switch>enable
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

Solo se debe confirmar presionando Enter.

Switch#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]

Tal y como en las otras veces, se presiona Enter para confirmar.

Ahora se vuelven a cargar ambos switches:

Switch#reload
Proceed with reload? [confirm]

Ahora verificaremos que la base de datos de vlan, no haya quedado en la memoria flash:

Switch>enable
Switch#show flash

Una vez ingresado este comando, desplegara una tabla y nos aseguraremos de que el archivo vlan.dat no aparezca.

3.2 PARTE 2: CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS

3.2.1 Paso 1: configurar la computadora de internet

Primero le asignaremos la dirección IPv4 en la casilla correspondiente, quedara así:

209.165.200.229

Ahora se asignará la máscara de subred, la cual será:

255.255.255.248

En el espacio de Gateway, se le asignará como Gateway predeterminado la:

209.165.200.225

Ahora asignamos la dirección IPv6 con su máscara:

2001:DB8:ACAD:A::38/64

Luego asignamos su Gateway predeterminada:

2001:DB8:ACAD:2::1

3.2.2 PASO 2: CONFIGURAR R1

Primero desactivaremos la búsqueda DNS, con los comandos:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
```

Ahora agregamos un nombre a nuestro router en este caso será R1:

```
Router(config)#hostname R1
R1(config)#
```

Agregaremos una contraseña de exec privilegiado cifrada (la contraseña será “class”):

```
R1(config)#enable secret class
```

Asignaremos una contraseña de acceso a la consola:

```
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
```

Ahora asignaremos una contraseña de acceso a Telnet:

```
R1(config)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#login
```

R1(config-line)#exit

Ahora cifraremos las contraseñas de texto no cifrado:

R1(config)#service password-encryption

Configuraremos un mensaje MOTD:

R1(config)#banner motd #Se prohibe el acceso no autorizado#

Ahora configuraremos la interfaz serial 0/0/0.

Primero le vamos a establecer una descripción:

R1(config)#interface serial0/0/0
R1(config-if)#description Interfaz DCE conectada hacia el R2

Ahora estableceremos una dirección IPv4:

R1(config-if)#ip address 172.16.1.1 255.255.255.252

Ahora estableceremos una dirección IPv6:

R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64

Se añade una frecuencia de reloj de 128000:

R1(config-if)#clock rate 128000

Por último, se activa la interfaz:

R1(config-if)#no shutdown

Ahora configuraremos unas rutas predeterminadas.

Primero se configura la ruta predeterminada en IPv4:

R1(config-if)#ip route 0.0.0.0 0.0.0.0 se0/0/0

Ahora configuramos la ruta predeterminada en IPv6:

R1(config)#ipv6 route ::/0 se0/0/0

3.2.3 Paso 3: configurar r2

Primero desactivaremos la búsqueda DNS:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
```

Asignamos R2 como nombre para el router:

```
Router(config)#hostname R2
R2(config)#
```

Asignamos una contraseña de modo exec privilegiado cifrada:

```
R2(config)#enable secret class
```

Ahora asignamos una contraseña de acceso a la consola:

```
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
```

Ahora asignaremos una contraseña de acceso a Telnet:

```
R2(config)#line vty 0 15
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
```

Ahora cifraremos las contraseñas de texto no cifrado:

```
R2(config)#service password-encryption
```

Ahora habilitamos el servidor HTTP:

(el software no dejo agregar el comando en ninguno de los diferentes router con los que cuenta, al parecer es un problema del mismo softwware)

Configuraremos un mensaje MOTD:

```
R2(config)#banner motd #Se prohibe el acceso no autorizado#
```

Ahora configuraremos la interfaz serial 0/0/0

Primero vamos a establecer una descripción:

```
R2(config)#interface serial0/0/0
R2(config-if)#description Interfaz conectada hacia el R1
```

Asignaremos la siguiente dirección IPv4 disponible en la subred:

```
R2(config-if)#ip address 172.16.1.2 255.255.255.252
```

Asignaremos una dirección IPv6 a la misma interfaz:

```
R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64
```

Ahora activamos la interfaz y salimos de ella:

```
R2(config-if)#no shutdown
R2(config-if)#exit
```

Ahora configuraremos la interfaz serial 0/0/1

Establecemos una descripción:

```
R2(config)#interface serial0/0/1
R2(config-if)#description Interfaz DCE conectada al R3
```

Asignamos la primera dirección IPv4 disponible de la subred:

```
R2(config-if)#ip address 172.16.2.1 255.255.255.252
```

Ahora asignamos una dirección IPv6:

```
R2(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64
```

Establecemos la frecuencia de reloj en 128000:

```
R2(config-if)#clock rate 128000
```

Activamos la interfaz y salimos:

```
R2(config-if)#no shutdown
R2(config-if)#exit
```

Ahora configuraremos la interfaz G0/0 (simulación de internet)

Establecemos una descripción:

```
R2(config)#interface gigabitethernet0/0
R2(config-if)#description Interfaz de simulacion de internet
```

Agregamos la primera dirección IPv4 disponible en la subred:

```
R2(config-if)#ip address 209.165.200.225 255.255.255.248
```

Ahora agregamos la primera dirección disponible de la subred de IPv6:

```
R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64
```

Activamos la interfaz y salimos de ella:

```
R2(config-if)#no shutdown
R2(config-if)#exit
```

Ahora ingresamos a la interfaz loopback 0

Agregaremos una descripción:

```
R2(config)#interface loopback 0
R2(config-if)#description Servidor web simulado
```

Asignamos la dirección IPv4 y salimos:

```
R2(config-if)#ip address 10.10.10.10 255.255.255.255
R2(config-if)#exit
```

Ahora configuraremos la ruta predeterminada de IPv4 e IPv6 por medio de G0/0:

```
R2(config)#ip route 0.0.0.0 0.0.0.0 gigabitethernet0/0
R2(config)#ipv6 route ::/0 gigabitethernet0/0
```

3.2.4 Paso 4: configurar R3

Primero desactivaremos la búsqueda DNS, con los comandos:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
```

Ahora agregamos un nombre a nuestro router en este caso será R3:

```
Router(config)#hostname R3
R3(config)#
```

Agregaremos una contraseña de exec privilegiado cifrada (la contraseña será “class”):

```
R3(config)#enable secret class
```

Asignaremos una contraseña de acceso a la consola:

```
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
```

Ahora asignaremos una contraseña de acceso a Telnet:

```
R3(config)#line vty 0 15
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
```

Ahora cifraremos las contraseñas de texto no cifrado:

```
R3(config)#service password-encryption
```

Configuraremos un mensaje MOTD:

```
R3(config)#banner motd #Se prohibe el acceso no autorizado#
```

Ahora ingresamos a la interfaz serial0/0/1 y agregamos una descripción:

```
R3(config)#interface serial 0/0/1
R3(config-if)#description Interfaz conectada a R2
```

Asignamos la siguiente dirección IPv4 de la subred:

```
R3(config-if)#ip address 172.16.2.2 255.255.255.252
```

Agregamos una IPv6 a la misma interfaz:

```
R3(config-if)#IPV6 address 2001:DB8:ACAD:2::2/64
```

Activamos la interfaz y salimos:

```
R3(config-if)#no shutdown
R3(config-if)#exit
```

Ahora ingresamos a la interfaz loopback 4 y asignamos la primera IPv4 disponible en la subred y salimos:

```
R3(config)#interface loopback 4
R3(config-if)#ip address 192.168.4.1 255.255.255.0
R3(config-if)#exit
```

Ahora ingresamos a la interfaz loopback 5 y asignamos la primera IPv4 disponible en la subred y salimos:

```
R3(config)#interface loopback 5
R3(config-if)#ip address 192.168.5.1 255.255.255.0
R3(config-if)#exit
```

Ahora ingresamos a la interfaz loopback 6 y asignamos la primera IPv4 disponible en la subred y salimos:

```
R3(config)#interface loopback 6
R3(config-if)#ip address 192.168.6.1 255.255.255.0
R3(config-if)#exit
```

Ahora ingresamos a la interfaz loopback 7 y asignamos una IPv6 y salimos:

```
R3(config)#interface loopback 7
R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64
R3(config-if)#exit
```

Ahora asignamos rutas prederterminadas IPv4 e IPv6 por la serial0/0/1:

```
R3(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/1
R3(config)#ipv6 route ::/0 serial0/0/1
```

3.2.5 Paso 5: configurar S1

Desactivaremos la búsqueda DNS:

```
Switch>enable
Switch#configure terminal
Switch(config)#no ip domain-lookup
```

Asignamos S1 como nombre del Switch:

```
Switch(config)#hostname S1
S1(config)#
```

Agregaremos una contraseña de exec privilegiado cifrada (la contraseña será “class”):

```
S1(config)#enable secret class
```

Asignaremos una contraseña de acceso a la consola:

```
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
```

Ahora asignaremos una contraseña de acceso a Telnet:

```
S1(config)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
```

Ahora cifraremos las contraseñas de texto no cifrado:

```
S1(config)#service password-encryption
```

Configuraremos un mensaje MOTD:

S1(config)#banner motd #Se prohibe el acceso no autorizado#

3.2.6 Paso 6: Configurar S3

Desactivaremos la búsqueda DNS:

Switch>enable
Switch#configure terminal
Switch(config)#no ip domain-lookup

Asignamos S3 como nombre del Switch:

Switch(config)#hostname S3
S3(config)#

Agregaremos una contraseña de exec privilegiado cifrada (la contraseña será “class”):

S3(config)#enable secret class

Asignaremos una contraseña de acceso a la consola:

S3(config)#line console 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit

Ahora asignaremos una contraseña de acceso a Telnet:

S3(config)#line vty 0 15
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit

Ahora cifraremos las contraseñas de texto no cifrado:

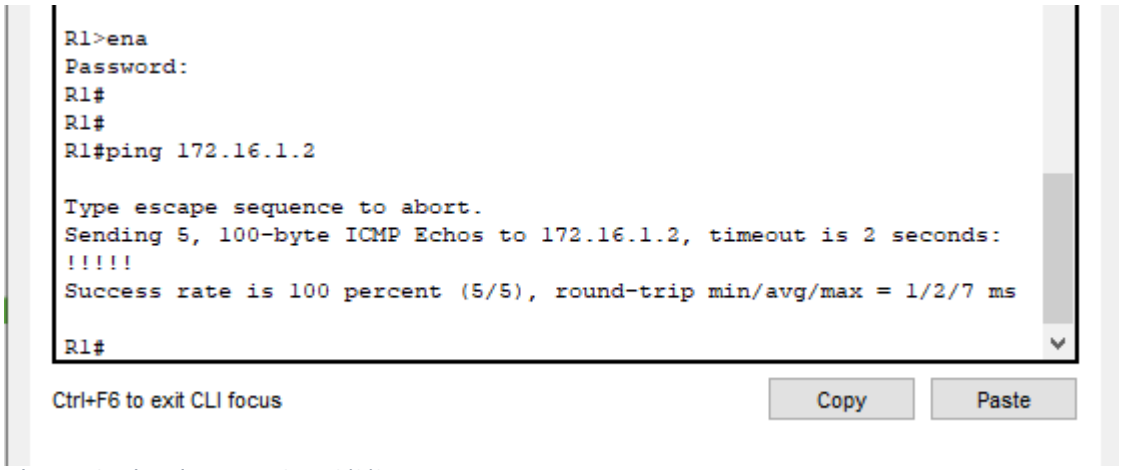
S3(config)#service password-encryption

Configuraremos un mensaje MOTD:

S3(config)#banner motd #Se prohibe el acceso no autorizado#

3.2.7 PASO 7: Verificar la conectividad de la red

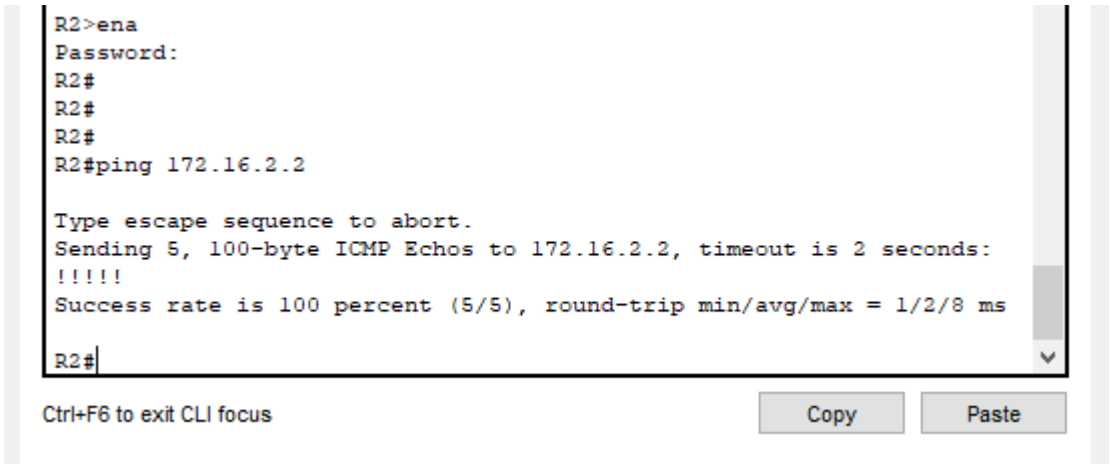
Primero se comprobará el ping Ipv4 del R1 al R2 en la interfaz serial 0/0/0



Figuras 2. ping de R1 a R2, se0/0/0

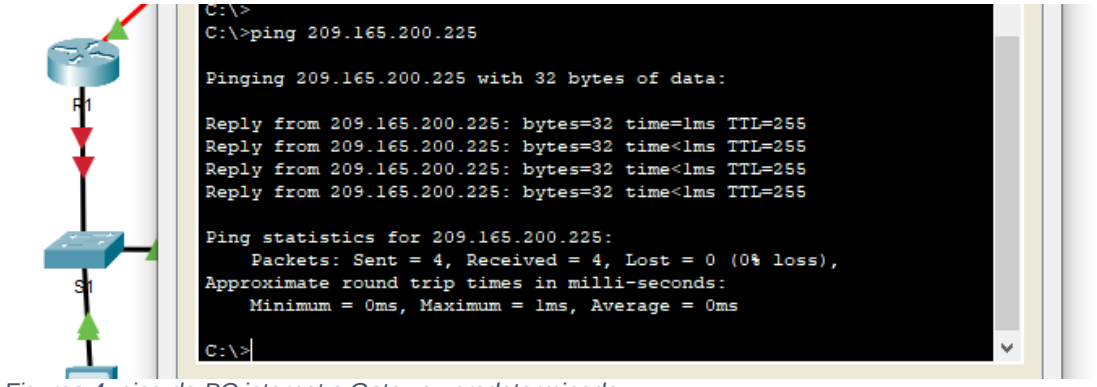
El ping ha salido exitoso.

Ahora se realizará un ping IPv4 del R2 al R3 en la inter serial 0/0/1



Figuras 3. ping de R2 a R3, se0/0/1

Ahora se realiza un ping, desde el PC internet, hasta su Gateway predeterminada.



Figuras 4. ping de PC internet a Gateway predeterminada

Como se puede apreciar, el ping salió exitoso.

3.3 PARTE 3: CONFIGURAR LA SEGURIDAD DEL SWITCH, LAS VLAN Y EL ROUTING ENTRE VLAN

3.3.1 Paso 1: configurar s1

Primero crearemos una base de datos de VLAN, donde se crearán y nombrarán cada una de las VLAN indicadas:

```
S1>enable
Password:
S1#configure terminal
S1(config)#vlan 21
S1(config-vlan)#name Contabilidad
S1(config-vlan)#exit
S1(config)#vlan 23
S1(config-vlan)#name Ingenieria
S1(config-vlan)#exit
S1(config)#vlan 99
S1(config-vlan)#name Administracion
S1(config-vlan)#exit
```

Ahora asignaremos la dirección IP de administración, esta dirección será la que se indica en el diagrama de la guía:

```
S1(config)#interface vlan 99
S1(config-if)#
S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#exit
```

Asignamos el Gateway predeterminado, la cual será la primera dirección IPv4 de la subred:

```
S1(config)#ip default-gateway 192.168.99.1
```

Forzaremos el enlace truncal en la interfaz F0/3, utilizaremos la VLAN 1 como VLAN nativa:

```
S1(config)#interface fastethernet 0/3
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#exit
```

Forzaremos el enlace truncal en la interfaz F0/5, utilizaremos la VLAN 1 como VLAN nativa:

```
S1(config)#interface fastethernet 0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#exit
```

Configuraremos los puertos restantes, como puertos de acceso:

```
S1(config)#interface range fa0/1 , fa0/2 , fa0/4 , fa0/6-24 , gi0/1 , gi0/2
S1(config-if-range)#switchport mode access
S1(config-if-range)#exit
```

Asignaremos la interfaz fastethernet 0/6 a la vlan 21:

```
S1(config)#interface fastethernet 0/6
S1(config-if)#switchport access vlan 21
S1(config-if)#exit
```

Apagaremos todos los puertos sin usar:

Por defecto ya los puertos se encuentran apagados.

3.3.2 Paso 2: configurar S3

Primero crearemos una base de datos de VLAN, donde se crearán y nombrarán cada una de las VLAN indicadas:

```
S3>enable
Password:
S3#configure terminal
S3(config)#vlan 21
S3(config-vlan)#name Contabilidad
S3(config-vlan)#exit
S3(config)#vlan 23
S3(config-vlan)#name Ingenieria
S3(config-vlan)#exit
S3(config)#vlan 99
S3(config-vlan)#name Administracion
S3(config-vlan)#exit
```

Ahora asignaremos la dirección IP de administración, esta dirección será la que se indica en el diagrama de la guía:

```
S3(config)#interface vlan 99
S3(config-if)#
S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#exit
```

Asignamos el Gateway predeterminado, la cual será la primera dirección IPv4 de la subred:

```
S3(config)#ip default-gateway 192.168.99.1
```

Forzaremos el enlace truncal en la interfaz F0/3, utilizaremos la VLAN 1 como VLAN nativa:

```
S3(config)#interface fastethernet 0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
S3(config-if)#exit
```

Configuraremos los puertos restantes, como puertos de acceso:

```
S3(config)#interface range fa0/1-2 , fa0/4-24
S3(config-if-range)#exit
```

Asignaremos la interfaz fastethernet 0/18 a la vlan 23:

```
S3(config)#interface fastethernet 0/18
S3(config-if)#switchport access vlan 23
S3(config-if)#exit
```

Apagaremos todos los puertos sin usar:

Por defecto están apagados.

3.3.3 Paso 3: Configurar R1

Ahora configuraremos la subinterfaz 802.1Q.21 en la G0/1

Asignaremos una descripción:

```
R1>enable
Password:
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface gigabitethernet0/1.21
R1(config-subif)#description LAN de Contabilidad
```

Asignaremos la vlan 21:

```
R1(config-subif)#encapsulation dot1Q 21
```

Asignamos la primera dirección disponible de la vlan 21 y salimos:

```
R1(config-subif)#ip address 192.168.21.1 255.255.255.0
R1(config-subif)#exit
```

Ahora configuraremos la subinterfaz 802.1Q.23 en la G0/1

Asignaremos una descripción:

```
R1(config)#interface gigabitethernet0/1.23
R1(config-subif)#description LAN de Ingenieria
```

Asignaremos la vlan 23:

```
R1(config-subif)#encapsulation dot1Q 23
```

Asignamos la primera dirección disponible de la vlan 23 y salimos:

```
R1(config-subif)#ip address 192.168.23.1 255.255.255.0
R1(config-subif)#exit
```

Ahora configuraremos la subinterfaz 802.1Q.99 en la G0/1

Asignaremos una descripción:

```
R1(config)#interface gigabitethernet0/1.99
R1(config-subif)#description LAN de Administracion
```

Asignaremos la vlan 99:

```
R1(config-subif)#encapsulation dot1Q 99
```

Asignamos la primera dirección disponible de la vlan 99 y salimos:

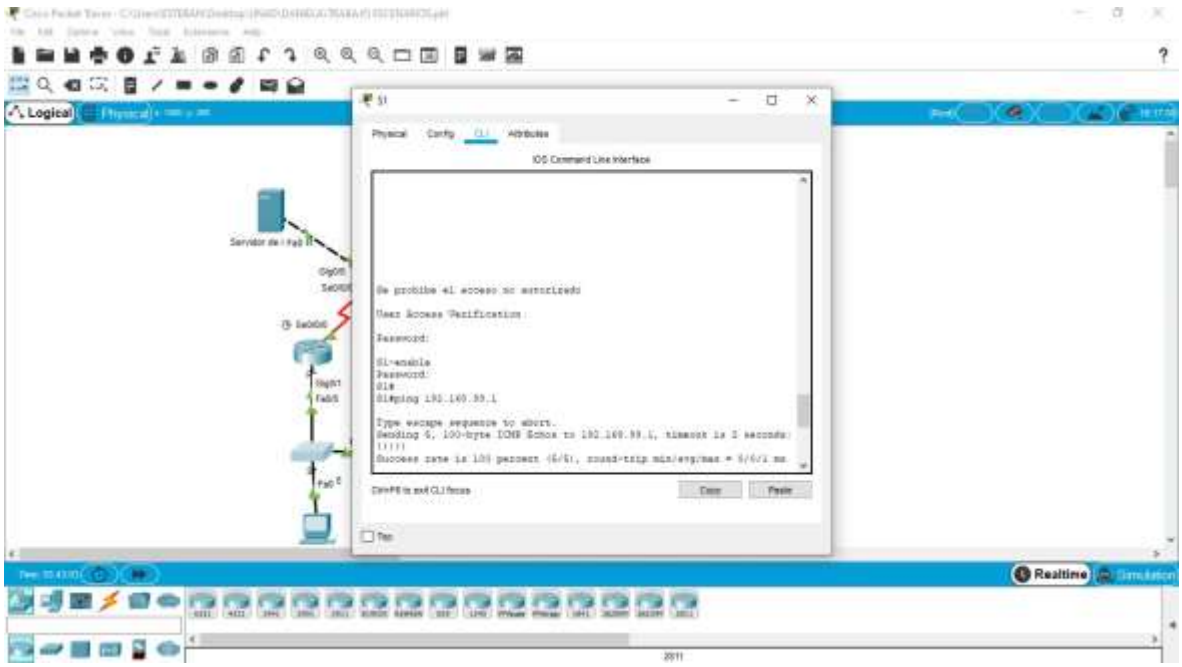
```
R1(config-subif)#ip address 192.168.99.1 255.255.255.0
R1(config-subif)#exit
```

Ingresamos a la interfaz G0/1 y la activamos:

```
R1(config)#interface gigabitethernet 0/1
R1(config-if)#no shutdown
```

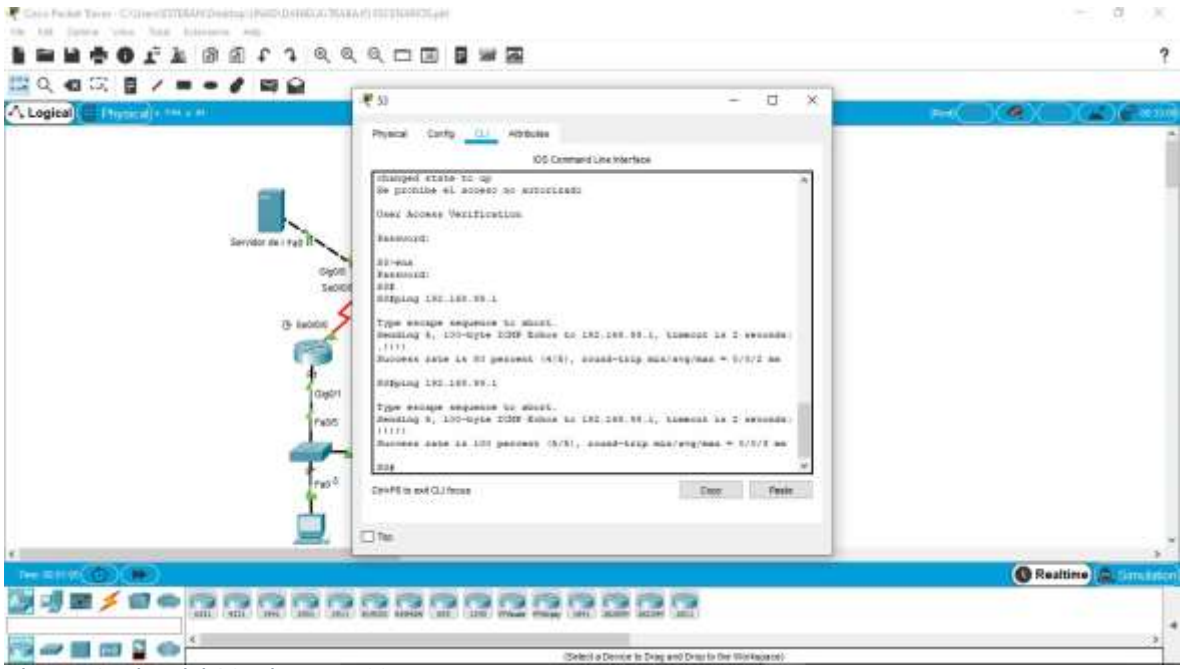
3.3.4 Paso 4: Verificar la conectividad de la red

Por medio del comando ping se probará la conectividad entre los Switch y el R1, el ping será hacía las direcciones vlan como se muestra en las siguientes imágenes:



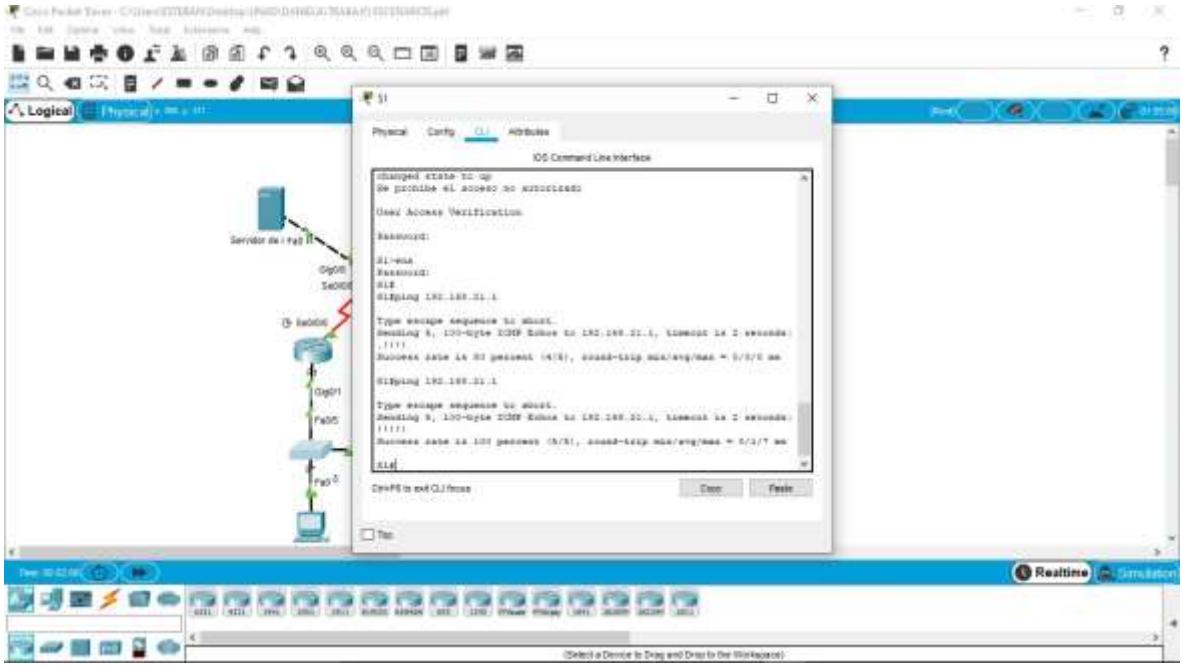
Figuras 5. Ping del S1 a la VLAN 99

El ping salió exitoso (todos los paquetes enviados).



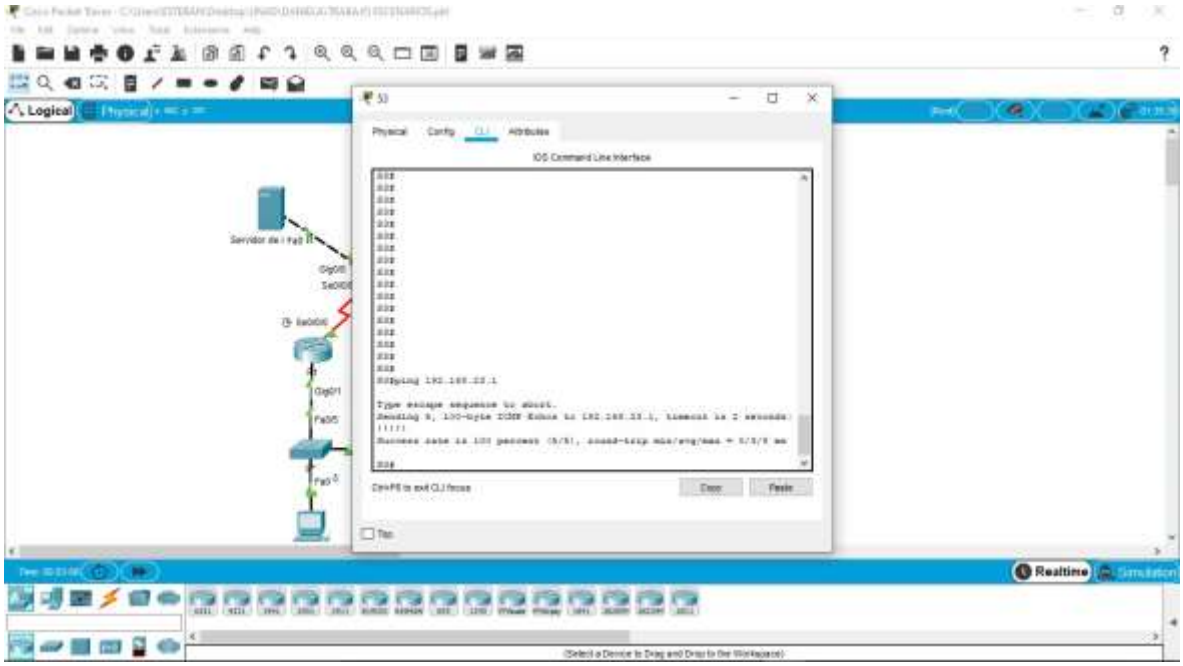
Figuras 6. Ping del S3 a la VLAN 99

El ping salió exitoso (todos los paquetes enviados).



Figuras 7. Ping del S1 a la VLAN 21

El ping salió exitoso (todos los paquetes enviados).



Figuras 8. Ping del S3 a la VLAN 23

El ping salió exitoso (todos los paquetes enviados)

3.4 PARTE 4: CONFIGURAR EL PROTOCOLO DE ROUTING DINÁMICO RIPV2

3.4.1 Paso 1: configurar ripv2 en el R1

Configuraremos el RIP versión 2:

```
R1>enable
Password:
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router rip
R1(config-router)#version 2
```

Anunciaremos las redes conectadas directamente:

```
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 172.16.1.0
R1(config-router)#network 192.168.99.0
R1(config-router)#network 192.168.23.0
R1(config-router)#network 192.168.21.0
```

Vamos a establecer todas las interfaces LAN como pasivas:

```
R1(config-router)#passive-interface gigabitethernet 0/0
R1(config-router)#passive-interface gigabitethernet 0/1
R1(config-router)#passive-interface gigabitethernet 0/2
R1(config-router)#passive-interface gigabitethernet 0/1.21
R1(config-router)#passive-interface gigabitethernet 0/1.23
R1(config-router)#passive-interface gigabitethernet 0/1.99
```

Desactivaremos la sumarización automática:

```
R1(config-router)#no auto-summary
```

3.4.2 Paso 2: configurar Ripv2 en el r2

Configuraremos RIP versión 2:

```
R2(config)#router rip
R2(config-router)#version 2
```

Anunciaremos las redes conectadas directamente, a excepción de la G0/0:

```
R2(config-router)#network 172.16.1.0
R2(config-router)#network 172.16.2.0
R2(config-router)#network 10.10.10.0
```

Estableceremos todas las LAN (loopback) como pasivas:

```
R2(config-router)#passive-interface loopback0
```

Desactivaremos la sumarización automática:

```
R2(config-router)#no auto-summary
```

3.4.3 Paso 3: configurar ripv2 en el R3

Primero configuraremos RIP versión 2:

```
R3(config)#router rip
R3(config-router)#version 2
```

Anunciaremos las redes IPv4 conectadas directamente:

```
R3(config-router)#network 172.16.2.0
R3(config-router)#network 192.168.4.0
R3(config-router)#network 192.168.5.0
R3(config-router)#network 192.168.6.0
```

Estableceremos todas la interface LAN IPv4 (Loopback) como pasivas:

```
R3(config-router)#passive-interface loopback4
R3(config-router)#passive-interface loopback5
R3(config-router)#passive-interface loopback6
```

Desactivaremos la sumarización automática:

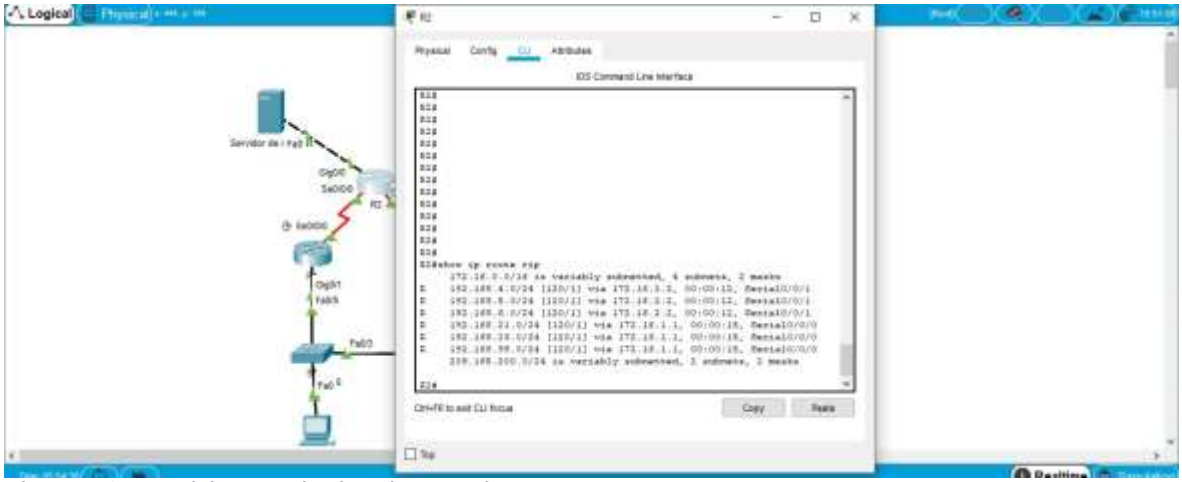
```
R3(config-router)#no auto-summary
```

3.4.4 Paso 4: verificar la información de RIP

Primero utilizaremos el comando “show ip protocols” para ver el ID del proceso RIP, la ID del router, las redes de routing y las interfaces pasivas configuradas en el R2:

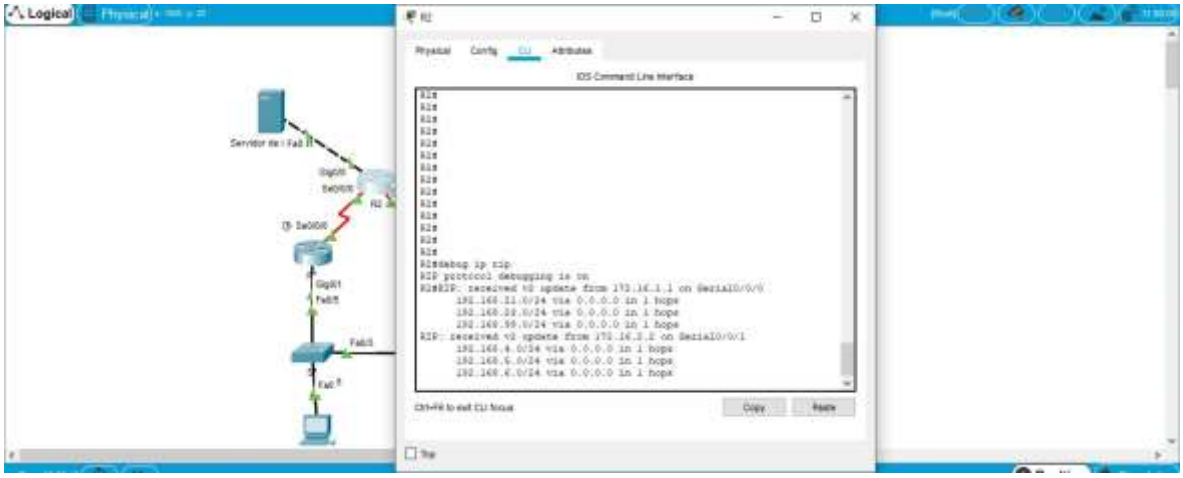
Figuras 9. Uso del comando show ip protocols

Ahora con el comando “show ip route rip” veremos solo las rutas RIP configuradas en el R2:



Figuras 10. Uso del comando show ip route rip

Con el comando “debug ip rip” veremos la sección de RIP en ejecución:



Figuras 11. Uso del comando debug ip route

3.5 PARTE 5: IMPLEMENTAR DHCP Y NAT PARA IPV4

3.5.1 Paso 1: configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Reservaremos las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas:

R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20

Reservaremos las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas:

R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20

Crearemos un pool de DHCP para la VLAN 21

Llamaremos al pool ACCT:

R1(config)#ip dhcp pool ACCT
R1(dhcp-config)#

Agregaremos el servidor DNS con dirección 10.10.10.10:

R1(dhcp-config)#dns-server 10.10.10.10

Agregaremos el nombre de dominio ccna-sa.com:

R1(dhcp-config)#domain-name ccna-sa.com

Agregaremos el Gateway predeterminado y salimos:

R1(dhcp-config)#network 192.168.21.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.21.1
R1(dhcp-config)#exit

Crearemos un pool de DHCP para la VLAN 23

Llamaremos al pool ENGNR:

R1(config)#ip dhcp pool ENGNR
R1(dhcp-config)#

Agregaremos el servidor DNS con dirección 10.10.10.10:

R1(dhcp-config)#dns-server 10.10.10.10

Agregaremos el nombre de dominio ccna-sa.com:

R1(dhcp-config)#domain-name ccna-sa.com

Agregaremos el Gateway predeterminado:

R1(dhcp-config)#network 192.168.23.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.21.1
R1(dhcp-config)#exit

3.5.2 Paso 2: Configurar la NAT estática y dinámica en el R2

Crearemos una base de datos local con una cuenta de usuario

Agregamos un nombre el cual será webuser, un nivel de privilegio 15 y una contraseña, la cual será cisco12345:

R2(config)#username webuser privilege 15 password cisco12345
R2(config)#line vty 0 15
R2(config-line)#login local

Habilitamos el servicio del servidor HTTP:

El software no permite ingresar el comando respectivo para el HTTP.

Configurar el servicio HTTP para utilizar la base de datos local para la autenticación:

El software no permite ingresar el comando respectivo para el HTTP

Crearemos una NAT estática al servidor web:

```
R2(config)#ip nat inside source static 192.168.21.0 209.165.200.229
R2(config)#ip nat inside source static 192.168.23.0 209.165.200.229
```

Asignaremos la interfaz interna y externa para la NAT estática:

```
R2(config)#interface gigabitethernet0/0
R2(config-if)#ip nat outside
R2(config-if)#exit
R2(config)#interface serial 0/0/0
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#interface serial 0/0/1
R2(config-if)#ip nat inside
R2(config-if)#exit
```

Configuraremos una NAT dinámica dentro de una ACL privada

Agregamos una lista de acceso registrada como 1, permitiremos la traducción de las redes de contabilidad y de ingeniería e R1, cada una con su wilcard:

```
R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255
```

Permitimos la traducción de un resumen de las redes LAN (loopback) en el R3

```
R2(config)#access-list 1 permit 192.168.0.0 0.0.7.255
```

Definiremos el pool de direcciones IP públicas utilizables, el nombre del pool será INTERNET y el conjunto de direcciones será 209.165.200.225-209.165.200.228:

```
R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask
255.255.255.0
```

Ahora definimos la traducción NAT dinámica:

```
R2(config)#ip nat inside source list 1 pool INTERNET
R2(config)#interface serial 0/0/0
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#interface serial 0/0/1
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#interface gigabitethernet 0/0
R2(config-if)#ip nat outside
R2(config-if)#exit
```

3.5.3 Paso 3: verificar el protocolo DHCP y la NAT estática

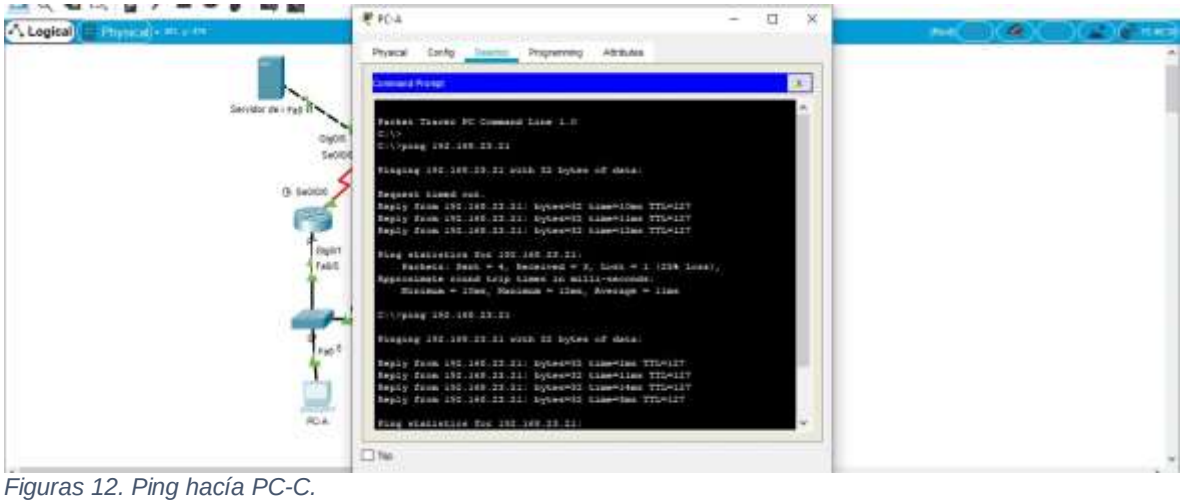
Verificaremos que la PC-A haya adquirido información de IP del servidor de DHCP:

Recibió la IP por DHCP exitosamente.

Verificaremos que la PC-C haya adquirido información de IP del servidor de DHCP:

Recibió la IP por DHCP exitosamente.

Verificaremos que la PC-A pueda hacer ping a la PC-C



Figuras 12. Ping hacía PC-C.

Utilizaremos un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**:

Si puede acceder a la página web, más no se puede comprobar si funciona el usuario y contraseña, debido a que, estas van vinculadas con el http y no se pudo activar ese servicio en el router.

3.6 PARTE 6: CONFIGURAR NTP

Primero ajustaremos la fecha y hora en el R2:

R2#clock set 19:16:00 9 may 2020

Configuraremos el R2 como maestro NTP:

R2(config)#ntp master 1

Configuraremos el R1 como un cliente NTP:

R1(config)#ntp server 172.16.1.2

Configuraremos R1 para actualizaciones de calendario periódicas con hora NTP:

R1(config)#ntp update-calendar

Verificaremos las configuraciones NTP en R1:

Figuras 13. Configuración NTP en R1

3.7 PARTE 7: CONFIGURAR Y VERIFICAR LAS LISTAS DE CONTROL DE ACCESO (ACL)

3.7.1 Paso 1: restringir el acceso a las líneas VTY en el R2

Configuraremos una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2:

```
R2(config)#ip access-list standar ADMIN-MGT
R2(config-std-nacl)#permit host 172.16.1.1
R2(config-std-nacl)#deny any
```

Aplicaremos la ACL con nombre a las líneas VTY:

```
R2(config)#line vty 0 15
```

Permitiremos el acceso por Telnet a las líneas VTY:

```
R2(config-line)#access-class ADMIN-MGT inR2(config-line)#access-class ADMIN-MGT in
```

Verificamos que la ACL funcione como se espera:

Si, se pudo conectar únicamente el R1 mientras que los demás hosts fueron rechazados.

3.7.2 Paso 2: Introducir el comando de CLI para mostrar lo siguiente

Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció:

```
Show Access-lists
```

Restablecer los contadores de una lista de acceso:

```
clear access-list counters <1-199>    o    clear access-list counters WORD
```

¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?:

```
Show ip interface
```

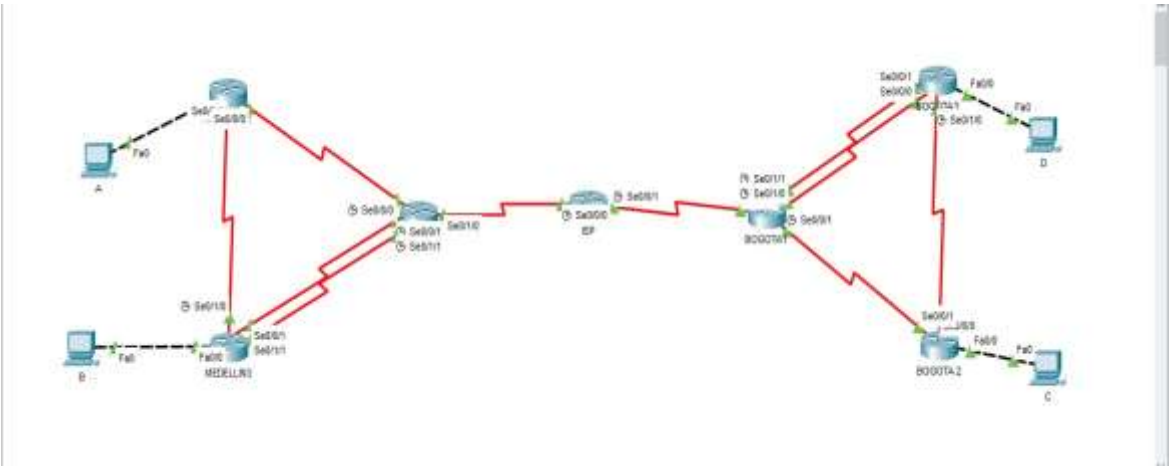
¿Con qué comando se muestran las traducciones NAT?:

show ip nat translations

¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?:

clear ip nat translation *

4. ESCENARIO 2



Figuras 14. Topología del escenario 2

PARTE 1: CONFIGURACIÓN DEL ENRUTAMIENTO

4.1.1 Configurar el enrutamiento en la red usando el protocolo OSPF versión 2, declare la red principal, desactive la sumarización automática.

4.1.1.1 ISP:

```
ISP>enable
ISP#configure terminal
ISP(config)#router ospf 1
ISP(config-router)#router-id 1.1.1.1
ISP(config-router)#network 209.17.220.0 0.0.0.3 area 1
ISP(config-router)#network 209.17.220.4 0.0.0.3 area 1
ISP (config-router)#exit
ISP(config)#ip default-network 209.17.220.0
```

4.1.1.2 MEDELLIN1:

```
MEDELLIN1>enable
MEDELLIN1#configure terminal
MEDELLIN1(config)#router ospf 1
MEDELLIN1(config-router)#router-id 2.2.2.2
MEDELLIN1(config-router)#network 209.17.220.0 0.0.0.3 area 1
MEDELLIN1(config-router)#network 172.29.6.0 0.0.0.3 area 1
MEDELLIN1(config-router)#network 172.29.6.8 0.0.0.3 area 1
MEDELLIN1(config-router)#network 172.29.6.12 0.0.0.3 area 1
MEDELLIN1(config-router)#exit
MEDELLIN1(config)#ip default-network 172.29.6.0
```

4.1.1.3 MEDELLIN2:

```
MEDELLIN2>enable
MEDELLIN2#configure terminal
MEDELLIN2(config)#router ospf 1
MEDELLIN2(config-router)#router-id 3.3.3.3
MEDELLIN2(config-router)#network 172.29.6.0 0.0.0.3 area 1
MEDELLIN2(config-router)#network 172.29.6.4 0.0.0.3 area 1
MEDELLIN2(config-router)#network 172.29.4.0 0.0.0.127 area 1
MEDELLIN2(config-router)#exit
MEDELLIN2(config)#ip default-network 172.29.6.0
```

4.1.1.4 MEDELLIN3:

```
MEDELLIN3>enable
MEDELLIN3#configure terminal
MEDELLIN3(config)#router ospf 1
MEDELLIN3(config-router)#router-id 4.4.4.4
MEDELLIN3(config-router)#network 172.29.6.12 0.0.0.3 area 1
MEDELLIN3(config-router)#network 172.29.6.8 0.0.0.3 area 1
MEDELLIN3(config-router)#network 172.29.6.4 0.0.0.3 area 1
MEDELLIN3(config-router)#network 172.29.4.128 0.0.0.127 area 1
MEDELLIN3(config-router)#exit
MEDELLIN3(config)#ip default-network 172.29.6.0
```

4.1.1.5 BOGOTA1:

```
BOGOTA1>enable
BOGOTA1#configure terminal
BOGOTA1(config)#router ospf 1
BOGOTA1(config-router)#router-id 5.5.5.5
```

```
BOGOTA1(config-router)#network 209.17.220.4 0.0.0.3 area 1
BOGOTA1(config-router)#network 172.29.3.0 0.0.0.3 area 1
BOGOTA1(config-router)#network 172.29.3.4 0.0.0.3 area 1
BOGOTA1(config-router)#network 172.29.3.8 0.0.0.3 area 1
BOGOTA1(config-router)#exit
BOGOTA1(config)#ip default-network 172.29.3.0
```

4.1.1.6 BOGOTA2:

```
BOGOTA2>enable
BOGOTA2#configure terminal
BOGOTA2(config)#router ospf 1
BOGOTA2(config-router)#router-id 6.6.6.6
BOGOTA2(config-router)#network 172.29.3.8 0.0.0.3 area 1
BOGOTA2(config-router)#network 172.29.3.12 0.0.0.3 area 1
BOGOTA2(config-router)#network 172.29.1.0 0.0.0.255 area 1
BOGOTA2(config-router)#exit
BOGOTA2(config)#ip default-network 172.29.3.0
```

4.1.1.7 BOGOTA3:

```
BOGOTA3>enable
BOGOTA3#configure terminal
BOGOTA3(config)#router ospf 1
BOGOTA3(config-router)#router-id 7.7.7.7
BOGOTA3(config-router)#network 172.29.3.0 0.0.0.3 area 1
BOGOTA3(config-router)#network 172.29.3.4 0.0.0.3 area 1
BOGOTA3(config-router)#network 172.29.3.12 0.0.0.3 area 1
BOGOTA3(config-router)#network 172.29.0.0 0.0.0.255 area 1
BOGOTA3(config-router)#exit
BOGOTA3(config)#ip default-network 172.29.3.0
```

4.1.2 Los routers Bogota1 y Medellín deberán añadir a su configuración de enrutamiento una ruta por defecto hacia el ISP y, a su vez, redistribuirla dentro de las publicaciones de OSPF.

4.1.2.1 BOGOTA1:

```
BOGOTA1(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/0
BOGOTA1(config)#router ospf 1
BOGOTA1(config-router)#default-information originate
BOGOTA1(config-router)# redistribute connected subnets tag 1
```

4.1.2.2 MEDELLIN1:

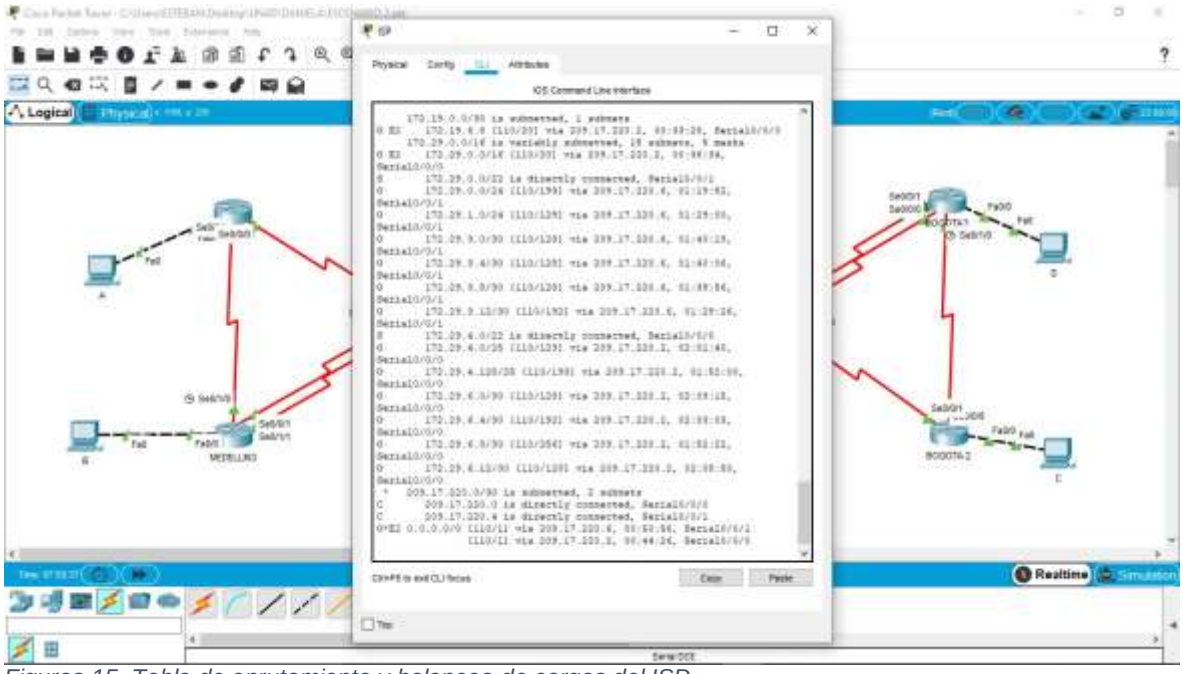
```
MEDELLIN1(config)#ip route 0.0.0.0 0.0.0.0 serial 0/1/0
MEDELLIN1(config)#router ospf 1
MEDELLIN1(config-router)#default-information originate
MEDELLIN1(config-router)#redistribute connected subnets tag 1
```

4.1.3 El router ISP deberá tener una ruta estática dirigida hacia cada red interna de Bogotá y Medellín para el caso se sumarizan las subredes de cada uno a /22.

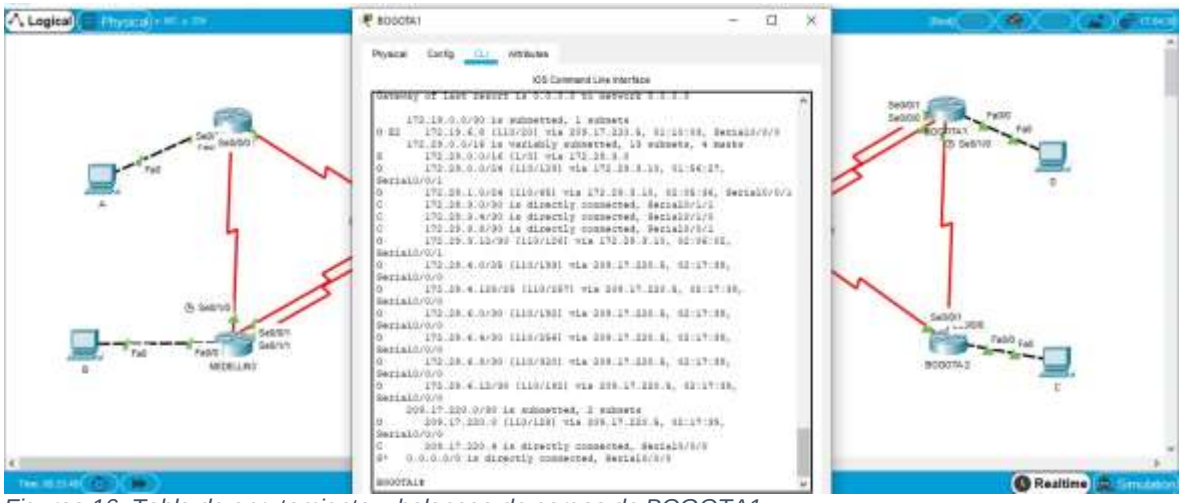
```
ISP(config)#ip route 172.29.4.0 255.255.252.0 serial 0/0/0
ISP(config)#ip route 172.29.0.0 255.255.252.0 serial 0/0/1
```

4.2 PARTE 2: TABLA DE ENRUTAMIENTO.

4.2.1 Verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas con balanceo de cargas.



Figuras 15. Tabla de enrutamiento y balanceo de cargas del ISP



Figuras 16. Tabla de enrutamiento y balanceo de cargas de BOGOTA1

Figuras 17. Tabla de enrutamiento y balanceo de cargas de BOGOTA2

Figuras 18. Tabla de enrutamiento y balanceo de cargas de BOGOTA3

Figuras 19. Tabla de enrutamiento y balanceo de cargas de MEDELLIN1

Figuras 20. Tabla de enrutamiento y balanceo de cargas de MEDELLIN2

Figuras 21. Tabla de enrutamiento y balanceo de cargas de MEDELLIN3

4.3 PARTE 3: DESHABILITAR LA PROPAGACIÓN DEL PROTOCOLO OSPF

4.3.1 Para no propagar las publicaciones por interfaces que no lo requieran se debe deshabilitar la propagación del protocolo OSPF.

MEDELLIN1:

```
MEDELLIN1(config)#router ospf 1
MEDELLIN1(config-router)#passive-interface fastethernet0/0
MEDELLIN1(config-router)#passive-interface fastethernet0/1
MEDELLIN1(config-router)#exit
```

4.3.1.1 MEDELLIN2:

```
MEDELLIN2(config)#router ospf 1
MEDELLIN2(config-router)#passive-interface fastethernet0/0
MEDELLIN2(config-router)#passive-interface fastethernet0/1
MEDELLIN2(config-router)#exit
```

MEDELLIN3:

```
MEDELLIN3(config)#router ospf 1
MEDELLIN3(config-router)#passive-interface fastethernet0/0
MEDELLIN3(config-router)#passive-interface fastethernet0/1
MEDELLIN3(config-router)#passive-interface serial0/0/0
MEDELLIN3(config-router)#exit
```

4.3.1.2 BOGOTA1:

```
BOGOTA1(config)#router ospf 1
BOGOTA1(config-router)#passive-interface fastethernet0/0
BOGOTA1(config-router)#passive-interface fastethernet0/1
BOGOTA1(config-router)#exit
```

4.3.1.3 BOGOTA2:

```
BOGOTA2(config)#router ospf 1
BOGOTA2(config-router)#passive-interface fastethernet0/0
BOGOTA2(config-router)#passive-interface fastethernet0/1
BOGOTA2(config-router)#exit
```

4.3.1.4 BOGOTA3:

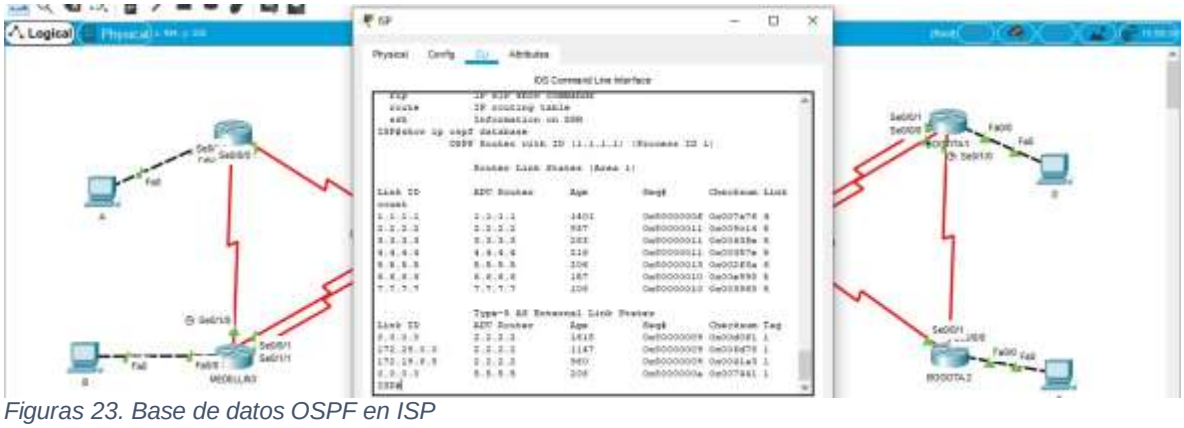
```
BOGOTA3(config)#router ospf 1
BOGOTA3(config-router)#passive-interface fastethernet0/0
BOGOTA3(config-router)#passive-interface fastethernet0/1
BOGOTA3(config-router)#passive-interface serial0/0/1
BOGOTA3(config-router)#exitg
```

4.4 PARTE 4: VERIFICACIÓN DEL PROTOCOLO OSPF

4.4.1 Verificar y documentar las opciones de enrutamiento configuradas en los routers, como el passive interface para la conexión hacia el ISP, la versión de OSPF y las interfaces que participan de la publicación entre otros datos.

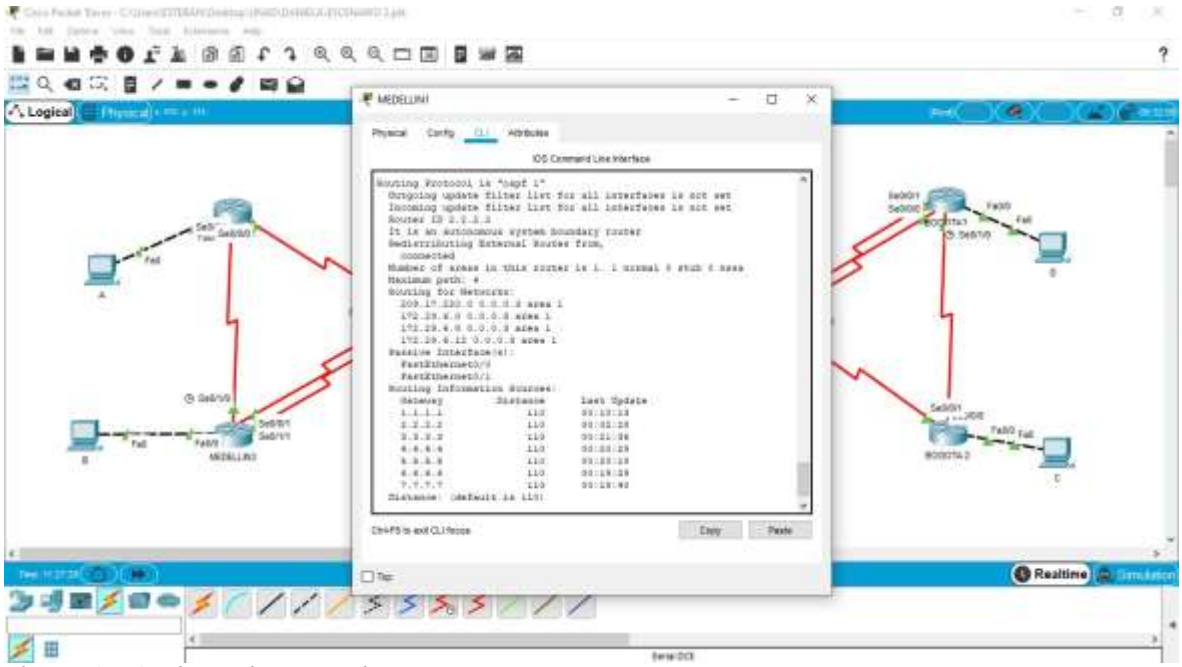
4.4.1.1 ISP:

Figuras 22. Opciones de enrutamiento en el ISP

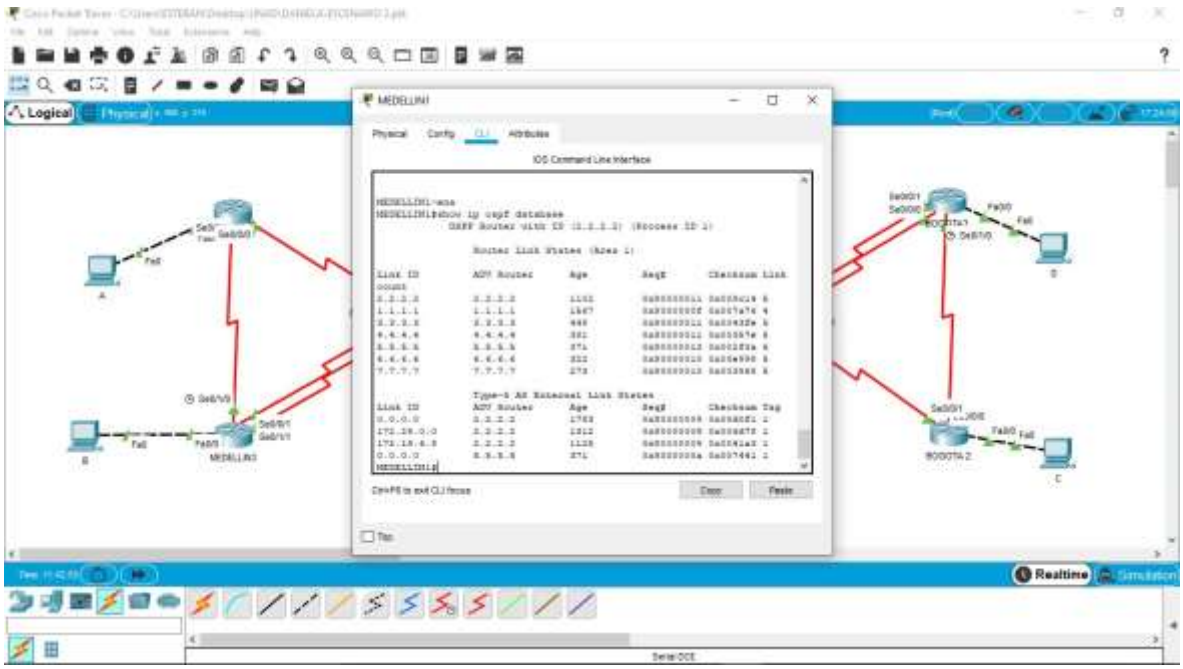


Figuras 23. Base de datos OSPF en ISP

4.4.1.2 MEDELLIN1:

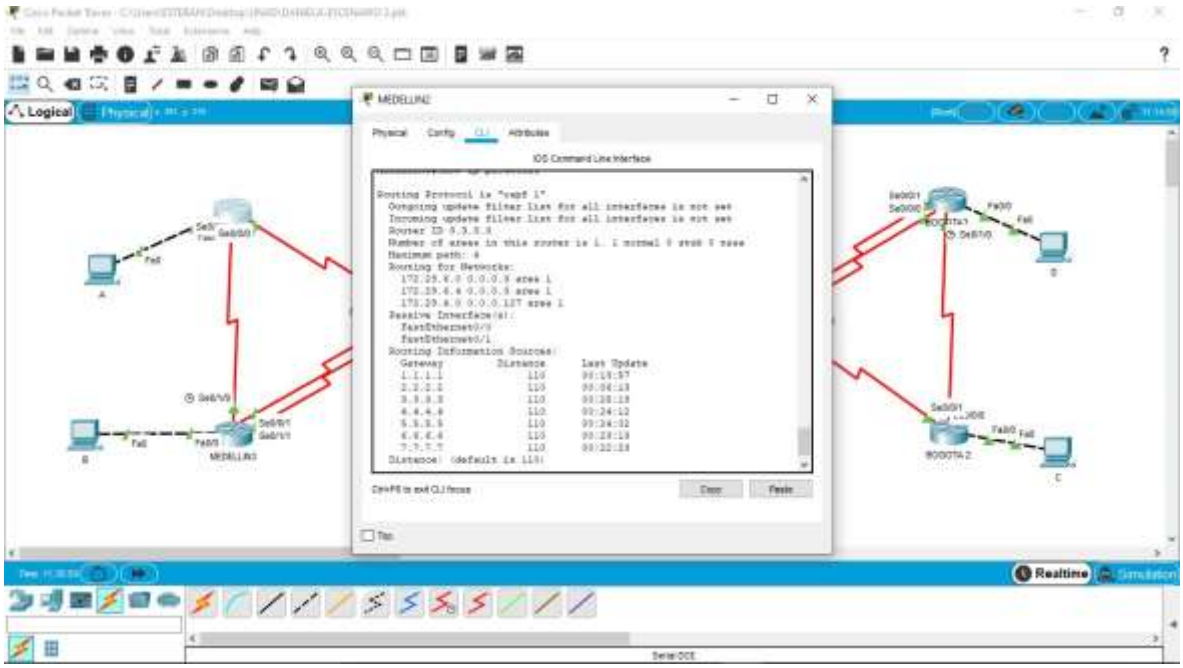


Figuras 24. Opciones de enrutamiento en MEDELLIN1

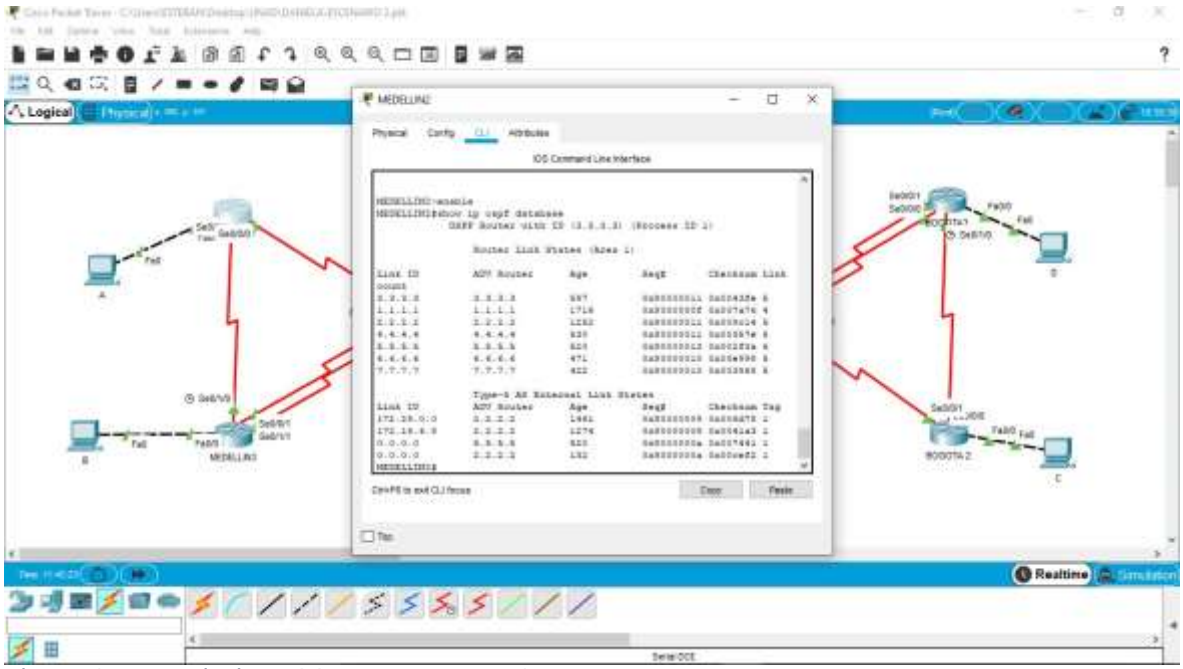


Figuras 25. Base de datos OSPF en MEDELLIN1

4.4.1.3 MEDELLIN2:

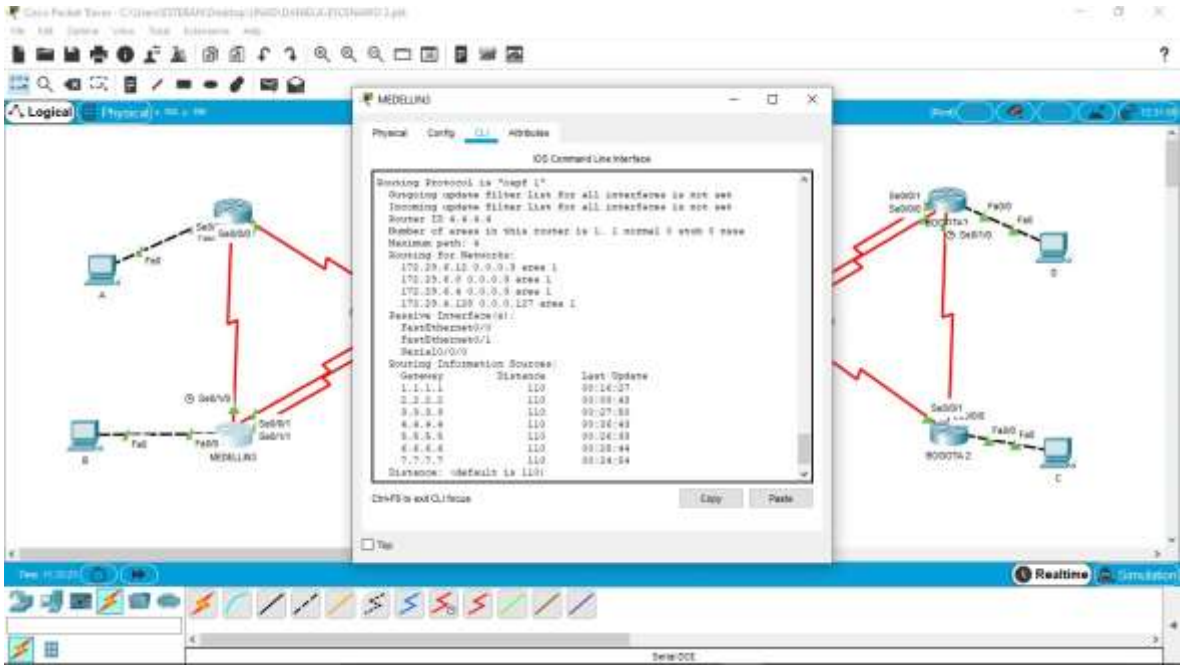


Figuras 26. Opciones de enrutamiento en MEDELLIN2

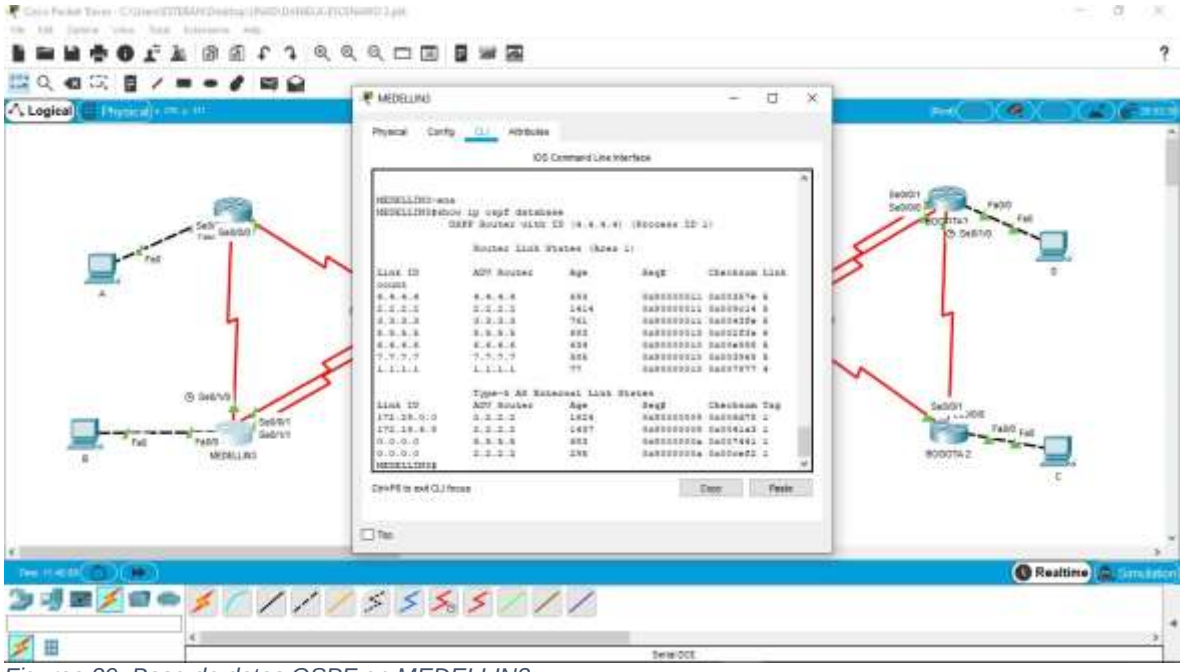


Figuras 27. Base de datos OSPF en MEDELLIN2

4.4.1.4 MEDELLIN3:

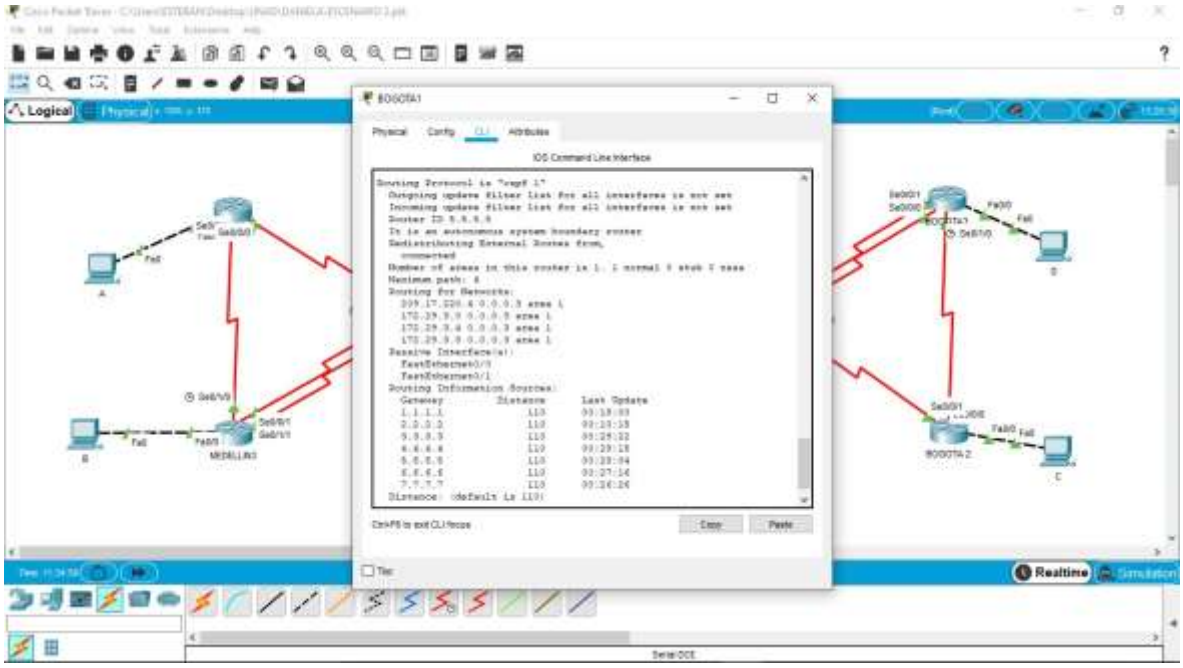


Figuras 28. Opciones de enrutamiento en MEDELLIN3

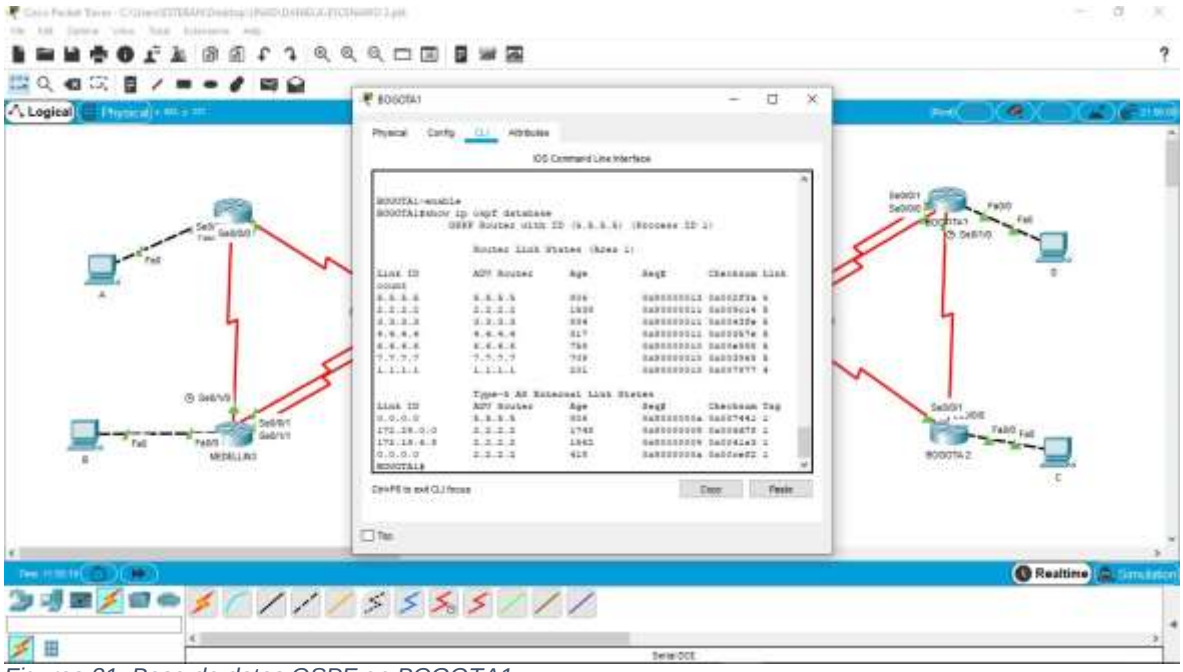


Figuras 29. Base de datos OSPF en MEDELLIN3

4.4.1.5 BOGOTA1:

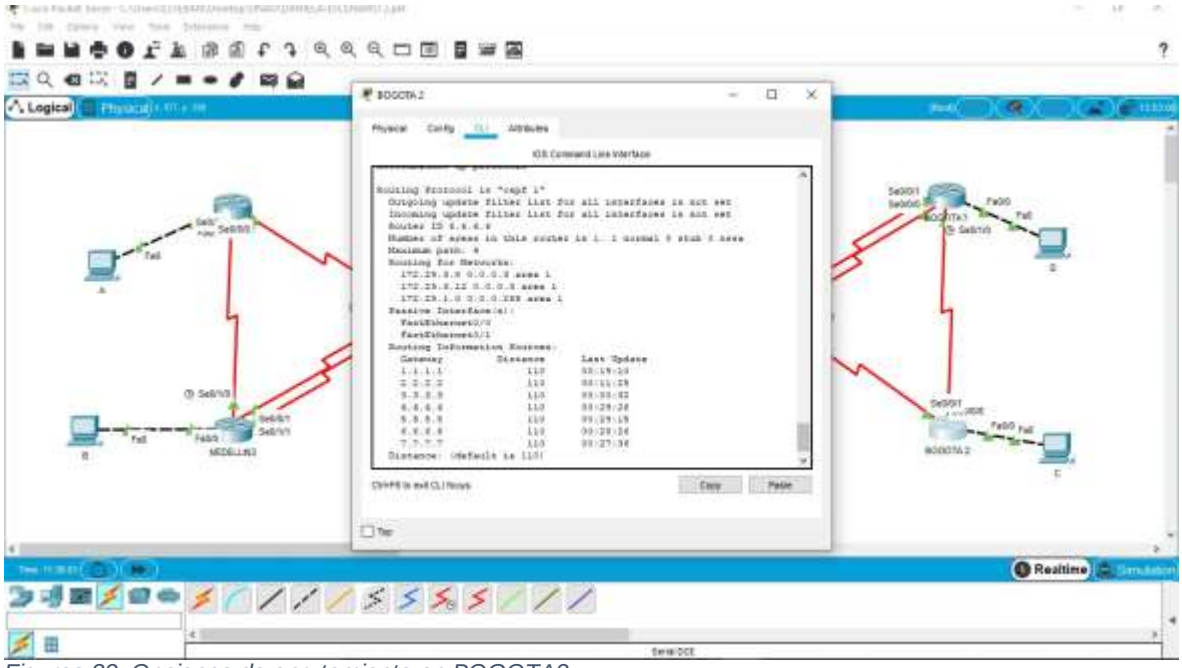


Figuras 30. Opciones de enrutamiento en BOGOTA1

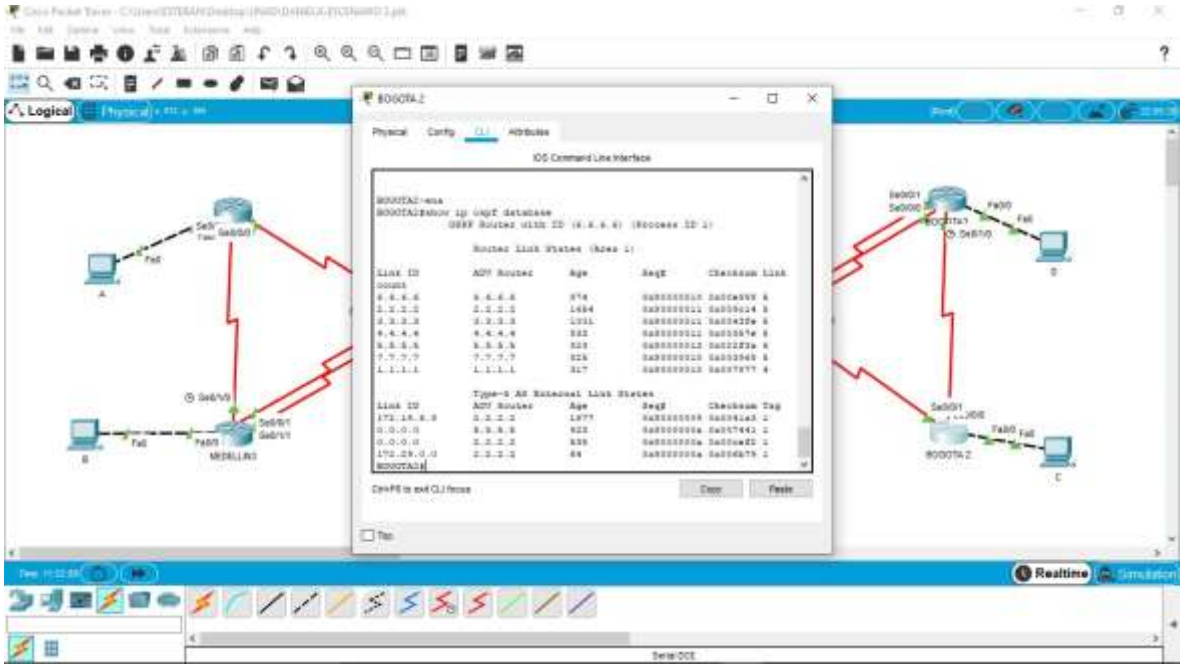


Figuras 31. Base de datos OSPF en BOGOTA1

4.4.1.6 BOGOTA2:

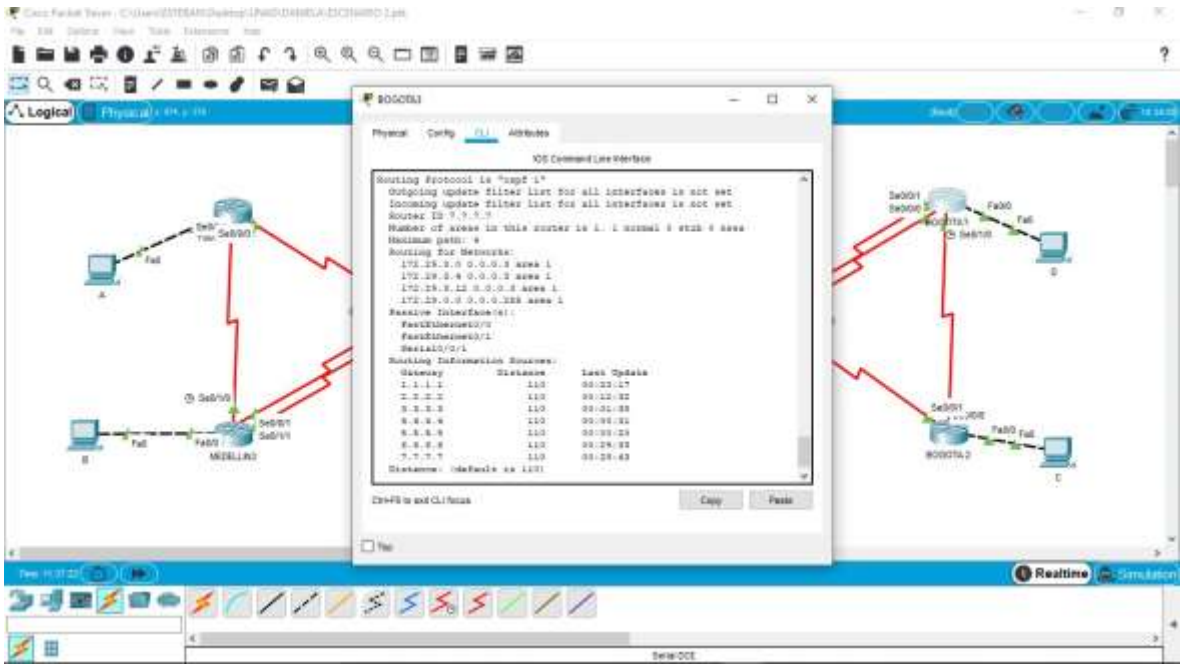


Figuras 32. Opciones de enrutamiento en BOGOTA2

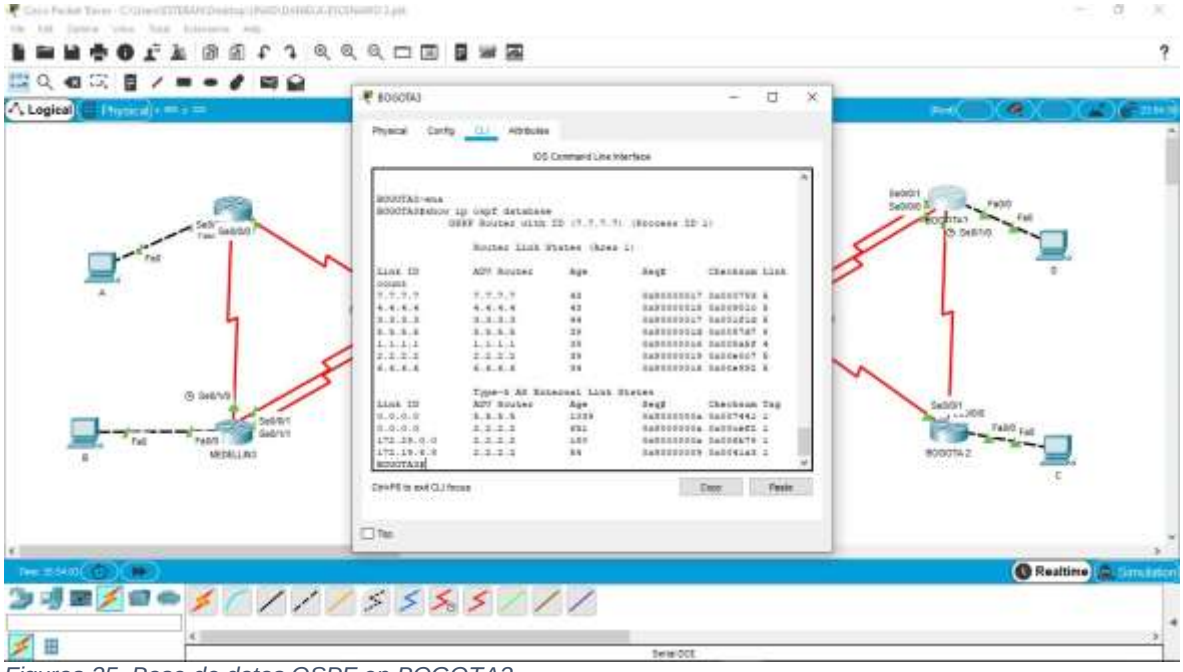


Figuras 33. Base de datos OSPF en BOGOTA2

4.4.1.7 BOGOTA3:



Figuras 34. Opciones de enrutamiento en BOGOTA3



Figuras 35. Base de datos OSPF en BOGOTA3

4.5 PARTE 5: CONFIGURAR ENCAPSULAMIENTO Y AUTENTICACIÓN PPP.

4.5.1 Según la topología se requiere que el enlace Medellín1 con ISP sea configurado con autenticación PAT.

4.5.1.1 MEDELLIN1:

```
MEDELLIN1(config)#username MEDELLIN1 password MEDELLIN1
MEDELLIN1(config)#interface serial 0/1/0
MEDELLIN1(config-if)#encapsulation ppp
MEDELLIN1(config-if)#ppp authentication pap
MEDELLIN1(config-if)#ppp pap sent-username ISP password ISP
MEDELLIN1(config-if)#exit
```

4.5.1.2 ISP:

```
ISP(config)#username ISP password ISP
ISP(config)#interface serial 0/0/0
ISP(config-if)#encapsulation ppp
ISP(config-if)#ppp authentication pap
ISP(config-if)#ppp pap sent-username MEDELLIN1 password MEDELLIN1
ISP(config-if)#exit
```

4.5.2 El enlace Bogotá1 con ISP se debe configurar con autenticación CHAT.

4.5.2.1 ISP:

```
ISP(config)#username BOGOTA1 password 12345
ISP(config)#interface serial 0/0/1
ISP(config-if)#encapsulation ppp
ISP(config-if)#ppp authentication chap
ISP(config-if)#exit
```

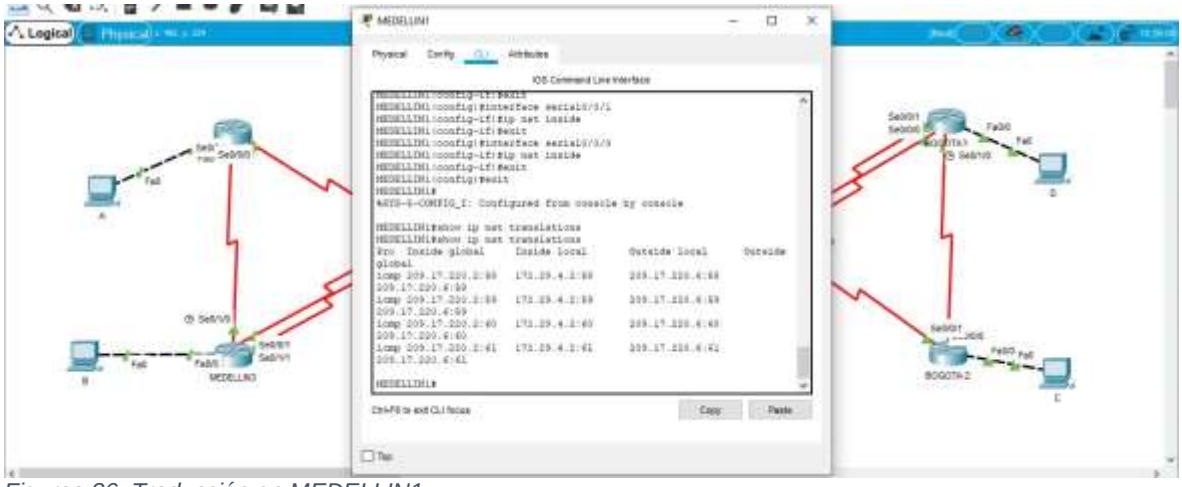
4.5.2.2 BOGOTA1:

```
BOGOTA1(config)#username ISP password 12345
BOGOTA1(config)#interface serial 0/0/0
BOGOTA1(config-if)#encapsulation ppp
BOGOTA1(config-if)#ppp authentication chap
BOGOTA1(config-if)#exit
```

4.6 PARTE 6: CONFIGURACIÓN DE PAT

4.6.1 Después de verificar lo indicado en el paso anterior proceda a configurar el NAT en el router Medellín1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Medellín1, cómo diferente puerto.

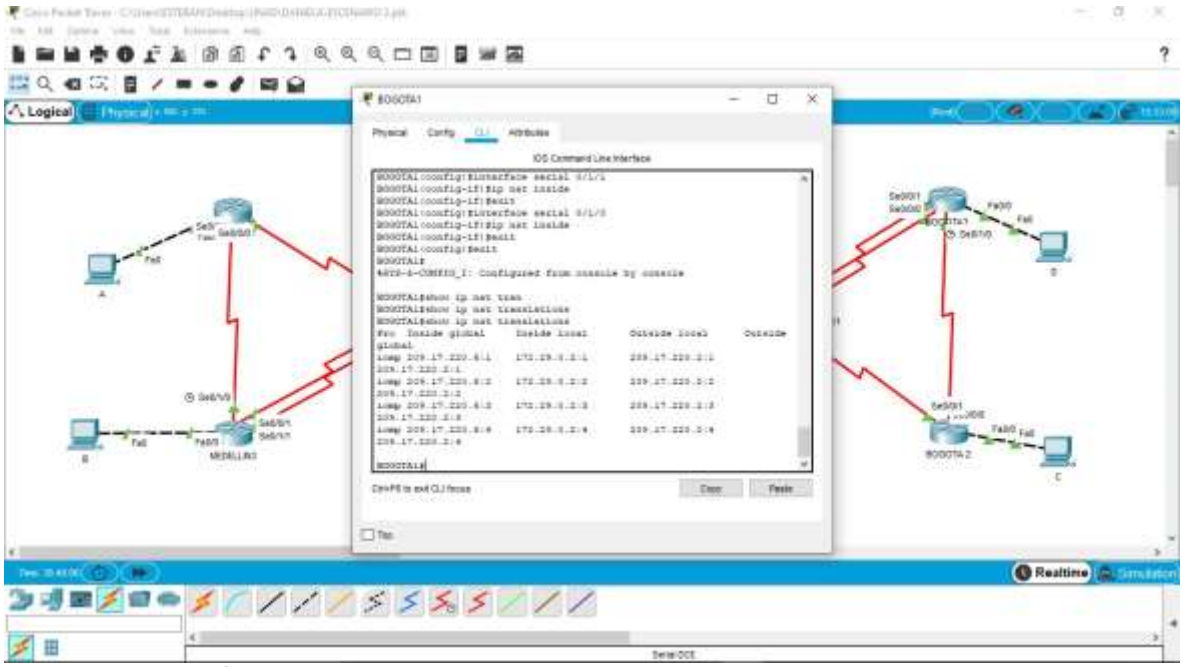
```
MEDELLIN1(config)#ip nat pool NAT1 209.17.220.1 209.17.220.2 netmask 255.255.255.252
MEDELLIN1(config)#access-list 1 permit 172.29.4.0 0.0.0.127
MEDELLIN1(config)#ip nat inside source list 1 pool NAT1
MEDELLIN1(config)#interface serial0/1/0
MEDELLIN1(config-if)#ip nat outside
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#interface serial0/1/1
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#interface serial0/0/1
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#interface serial0/0/0
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#exit
```



Figuras 36. Traducción en MEDELLIN1

4.6.2 Proceda a configurar el NAT en el router Bogotá1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Bogotá1, cómo diferente puerto.

```
BOGOTA1(config)#access-list 1 permit 172.29.0.0 0.0.0.127
BOGOTA1(config)#ip nat inside source list 1 pool NAT2
BOGOTA1(config)#interface serial 0/0/0
BOGOTA1(config-if)#ip nat outside
BOGOTA1(config-if)#exit
BOGOTA1(config)#interface serial 0/0/1
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#exit
BOGOTA1(config)#interface serial 0/1/1
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#exit
BOGOTA1(config)#interface serial 0/1/0
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#exit
```



Figuras 37.Traducción en BOGOTA1

4.7 PARTE 7: CONFIGURACIÓN DEL SERVICIO DHCP.

4.7.1 Configurar la red Medellín2 y Medellín3 donde el router Medellín 2 debe ser el servidor DHCP para ambas redes Lan.

```
MEDELLIN2(config)#ip dhcp pool MEDELLIN1
MEDELLIN2(dhcp-config)#exit
MEDELLIN2(config)#no ip dhcp pool MEDELLIN1
MEDELLIN2(config)#ip dhcp pool MEDELLIN2
MEDELLIN2(dhcp-config)#network 172.29.4.0 255.255.255.128
MEDELLIN2(dhcp-config)#default-router 172.29.4.1
MEDELLIN2(dhcp-config)#exit
MEDELLIN2(config)#ip dhcp pool MEDELLIN3
MEDELLIN2(dhcp-config)#network 172.29.4.128 255.255.255.128
MEDELLIN2(dhcp-config)#default-network 172.29.4.129
MEDELLIN2(dhcp-config)#default-router 172.29.4.129
MEDELLIN2(dhcp-config)#exit
```

4.7.2 El router Medellín3 deberá habilitar el paso de los mensajes broadcast hacia la IP del router Medellín2.

```
MEDELLIN3(config)#interface fastethernet0/0
MEDELLIN3(config-if)#ip helper-address 172.29.6.5
MEDELLIN3(config-if)#exit
```

4.7.3 Configurar la red Bogotá2 y Bogotá3 donde el router Medellín2 debe ser el servidor DHCP para ambas redes Lan.

```
MEDELLIN2(config)#ip dhcp pool BOGOTA2
MEDELLIN2(dhcp-config)#network 172.29.1.0 255.255.255.0
MEDELLIN2(dhcp-config)#default-router 172.29.1.1
MEDELLIN2(dhcp-config)#exit
MEDELLIN2(config)#ip dhcp pool BOGOTA3
MEDELLIN2(dhcp-config)#network 172.29.0.0 255.255.255.0
MEDELLIN2(dhcp-config)#default-router 172.29.0.1
MEDELLIN2(dhcp-config)#exit
```

4.7.4 Configure el router Bogotá1 para que habilite el paso de los mensajes Broadcast hacia la IP del router Bogotá2

```
BOGOTA1(config)#interface serial 0/0/1
BOGOTA1(config-if)#ip helper-address 172.29.6.2
BOGOTA1(config-if)#exit
```

CONCLUSIONES

Al momento de configurar los distintos escenarios no hubo demasiados problemas para la configuración, uno de los pocos inconvenientes fueron en el escenario 1, a la hora de configurar la VLAN 23, debido a que la guía decía que se debía configurar esa VLAN, cuando esto era incorrecto, cuando se fue a realizar el ping a determinada VLAN presente un fallo y rechazó el ping; para darle solución se tuvo que revisar nuevamente la configuración y se analizó con la guía, sin embargo todo concordaba, al momento de revisar la topología se vio que la VLAN configurada en el S3 no era la misma que en la topología; por ello se configuró nuevamente la interfaz que pertenecía a la VLAN 23 en el S3 y se realizó un nuevo ping, en el cual toda fue exitoso. Otro caso fue el de activar el servicio HTTP en un router, el software de simulación no permitió realizar esto para la configuración, sin embargo, esto no representó un problema para más configuraciones.

En el escenario 2 se presentó el inconveniente de desactivar la sumarización automática, para este caso era necesario desactivarla según lo indicado, pero en el protocolo OSPF no es necesario o por lo menos no brinda la opción para hacerlo; aquí también se siguieron todas las indicaciones brindadas y no hubo problema a la hora de configurar, hacer ping u otros comandos.

BIBLIOGRAFÍAS

CCNA Routing and Switching: Introducción a las redes (Introduction to Networks). Capítulo 7: Direccionamiento IP. Recuperado de https://1314297.netacad.com/courses/973101/modules/items/65159037

CCNA Routing and Switching: Introducción a las redes (Introduction to Networks). Capítulo 8: División de redes IP en subredes .Recuperado de https://1314297.netacad.com/courses/973101/modules/items/65159041

CCNA Routing and Switching: Introducción a las redes (Introduction to Networks). Capítulo 9: Capa de transporte. Recuperado de https://1314297.netacad.com/courses/973101/modules/items/65159046

CCNA Routing and Switching: Introducción a las redes (Introduction to Networks). Capítulo 10: Capa de aplicación. Recuperado de https://1314297.netacad.com/courses/973101/modules/items/65159050

CCNA Routing and Switching: Introducción a las redes (Introduction to Networks). Capítulo 11: Configuración de un sistema operativo de red. Recuperado de https://1314297.netacad.com/courses/973101/modules/items/65159054

CCNA Routing and Switching: Principios básicos de routing y switching. Capítulo7: Listas de acceso. Recuperado de https://1314297.netacad.com/courses/1003497/modules/items/66668554

CCNA Routing and Switching: Principios básicos de routing y switching. Capítulo 8: DHCP. Recuperado de https://1314297.netacad.com/courses/1003497/modules/items/66668559

CCNA Routing and Switching: Principios básicos de routing y switching. Capítulo 9: NAT para IPv4. Recuperado de https://1314297.netacad.com/courses/1003497/modules/items/66668563

CCNA Routing and Switching: Principios básicos de routing y switching. Capítulo 10: Detección, administración y mantenimiento de dispositivos. Recuperado de https://1314297.netacad.com/courses/1003497/modules/items/66668567